ISSN: 0716-7415 versión impresa
ISSN: 0719-8027 versión en línea
DOI: 10.26797
www.politicayestrategia.cl

Academia Nacional de Estudios
Políticos y Estratégicos

Revista Política y Estrategia

Nº 143 – ENERO - JUNIO 2024

Artículos

HACIA UNA PROPUESTA DE SEGURIDAD NACIONAL A LA LUZ DE LOS CASOS DE CHILE Y MÉXICO Y EL COMBATE AL CRIMEN ORGANIZADO
Diego Ramírez Sánchez

TERRORISMO EN ECUADOR; UN RETO PARA LAS FUERZAS ARMADAS PARA LA APLICACIÓN DE TÁCTICAS EN UNA GUERRA ASIMÉTRICA
Marlon F. Luna Quiroz - Ricardo J. Acuña López

LA INTELIGENCIA CRIMINAL: CONCEPTO, IMPLEMENTACIÓN, EXPERIENCIAS COMPARADAS
José Manuel Ugarte

AMENAZAS HÍBRIDAS Y LA POLÍTICA DE DEFENSA NACIONAL DE CHILE
Claudio Bertin Wiehoff

Estudios

DESCODIFICANDO LA INFRAESTRUCTURA CRÍTICA CASO NACIONAL
Fulvio Queirolo Pellerano

Dossier

EL ANUNCIO DE UN NUEVO ORDEN INTERNACIONAL

ANNUAL THREAT ASSESSMENT OF THE U.S. INTELLIGENCE COMMUNITY

CONFERENCIA DE SEGURIDAD DE MÚNICH: EL ALTO REPRESENTANTE JOSEP BORRELL SOBRE LA NUEVA AGENDA GEOPOLÍTICA

Reseñas

LIDERAZGO. SEIS ESTUDIOS SOBRE ESTRATEGIA MUNDIAL
Gonzalo Carrasco Astudillo

REVISTA

POLÍTICA Y ESTRATEGIA

www.politicayestrategia.cl

PUBLICACIÓN SEMESTRAL DE LA ACADEMIA NACIONAL DE ESTUDIOS POLÍTICOS Y ESTRATÉGICOS

Artículos
Estudios
Dossier
Reseñas

N°143

ENERO – JUNIO
2024

La Revista Política y Estrategia es una publicación de la Academia Nacional de Estudios Políticos y Estratégicos, ANEPE. Fundada en 1976 posee un carácter bianual. Su línea editorial está centrada en todos aquellos tópicos pertinentes y relevantes relativos a la Seguridad y Defensa con efectos a nivel nacional, regional y mundial, entre los que se encuentran asuntos políticos relacionados, amenazas a la paz y seguridad, pensamiento estratégico, transformaciones del escenario internacional, relaciones internacionales y derecho internacional.

La revista tiene su versión digital en el portal www.revistapoliticayestrategia.cl, está adscrita al Directorio DOAJ (Directorio de Revistas de Acceso Abierto) y al Directorio de Acceso Abierto para Recursos Académicos ROAD, cuenta con el sistema DOI de identificación de objeto digital para todos sus contenidos, a través del sistema Crossref, además ellos se publican bajo una licencia Creative Commons 4.0 Reconocimiento Internacional (CC BY 4.0).

La revista se encuentra disponible en el Sistema de Información en Línea para Revistas Científicas de América Latina, el Caribe, España y Portugal, Latindex (www.latindex.org/), así como en el Sistema de Información electrónica CLASE (Base de datos bibliográfica de revistas de ciencias sociales y humanidades), dependiente de la Universidad Nacional Autónoma de México (UNAM). Sus contenidos se divulgan en línea a través de internet y está disponible de manera gratuita en la página http://clase.unam.mx y en Dialnet, dependiente de la Universidad de La Rioja, España, http://dialnet.unirioja.es/servlet/revista?codigo=22331. Además es parte del Directorio REDIB (Red Iberoamericana de Innovación y Conocimiento Científico) (https://www.redib.org/) que es una plataforma de agregación de contenidos científicos y académicos en formato electrónico producidos en el ámbito iberoamericano.

Diagramación
Juan P. Bravo Zamora

Soporte Técnico Plataforma OJS
Óscar Sandoval Carlos

Publicación sitio web
Bernardita Alarcón Carvajal

La Revista Política y Estrategia se publica semestralmente y está registrada bajo el ISSN 0716-7415, en su versión impresa, e ISSN 0719-7415 en su versión en línea.

Dirección Postal: Avda. Eliodoro Yáñez 2760,
Providencia, Santiago, Chile.
Sitio web www.anepe.cl, https://rpye.anepe.cl
Teléfonos (56-2) 2598 1000, fax (56-2) 2598 1043
Correo electrónico rpye@anepe.cl

REVISTA

"POLÍTICA Y ESTRATEGIA"

SUMARIO

Editorial 9

Artículos

Hacia una propuesta de Seguridad Nacional a la luz de los casos de Chile y México y el combate al crimen organizado 13
Diego Ramírez Sánchez

Terrorismo en Ecuador; un reto para las Fuerzas Armadas para la aplicación de tácticas en una guerra asimétrica 39
Marlon F. Luna Quiroz - Ricardo J. Acuña López

La inteligencia criminal: concepto, implementación, experiencias comparadas 69
José Manuel Ugarte

Amenazas híbridas y la Política de Defensa Nacional de Chile 111
Claudio Bertin Wiehoff

Estudios

Descodificando la infraestructura crítica. Caso nacional 139
Fulvio Queirolo Pellerano

Dossier

El anuncio de un nuevo orden internacional 157
El Editor

Annual threat assessment of the U.S. intelligence community 179
El Editor

Conferencia de seguridad de Múnich: El Alto Representante Josep Borrell sobre la nueva agenda geopolítica 221
El Editor

Reseñas

Liderazgo. Seis estudios sobre estrategia mundial 229
Gonzalo Carrasco Astudillo

Revista "Política y Estrategia" Nº 143, 2024, pp. 9-10
ISSN 0716-7415 (versión impresa) - ISSN 0719-8027 (versión en línea)
Academia Nacional de Estudios Políticos y Estratégicos
Editorial

EDITORIAL

Desde el punto de vista del contexto internacional, nos encontramos con un año cargado de eventos electorales que inciden en el devenir político, económico y social de nuestra ya complicada aldea global que está acusando un problema de incertidumbre. Así, por ejemplo, de los resultados de la elección presidencial norteamericana que obviamente es la más importante, se verá si vuelve a predominar una versión aislacionista en política exterior con sus consiguientes efectos especialmente en relación a la OTAN y a China y Rusia o se mantendrá la apertura actual. Respecto de Europa, el reciente triunfo de la centroderecha en las elecciones del Parlamento Europeo en principio significaría la mantención de una visión europeísta en términos generales, pero el impacto del crecimiento electoral de la ultraderecha tal vez provocará cambios en algunos países tan importantes como Francia o Alemania. En nuestra región, la presidencia de México ha quedado en manos de la candidata oficialista, quien deberá enfrentar el grave problema de seguridad que afecta dicho país, así como también la situación migratoria considerando el endurecimiento de la política de los EE. UU. al respecto. En Centroamérica y el Cono Sur, junto a las limitaciones que todavía se observan en el plano de la economía y el proceso de desarrollo post COVID, no cabe duda de que la seguridad frente al flagelo del narcotráfico y el crimen organizado tiende a dominar la agenda de diferentes gobiernos, donde México y Ecuador aparecen como casos paradigmáticos. De esta manera, en el número actual de la revista, incorporamos cuatro artículos que giran en torno a la seguridad y defensa tanto en nuestro país como en la Región. El primero de ellos, se titula: *"Hacia una propuesta de Seguridad Nacional a la luz de los casos de Chile y México y el combate al crimen organizado"*; el segundo: *"Terrorismo en Ecuador; un reto para las Fuerzas Armadas para la aplicación de tácticas en una guerra asimétrica"*; el tercero: *"La inteligencia criminal: concepto, implementación, experiencias comparadas"*, y finalmente: *"Amenazas híbridas y la Política de Defensa Nacional de Chile".*

A continuación de los artículos, tenemos un ensayo denominado: *"Descodificando la infraestructura crítica: caso nacional",* que trata sobre un importante concepto en discusión dado que se relaciona con la posible participación de las FF. AA. en la protección de este tipo de bienes.

En la sección Dossier, hemos incluido tres documentos muy destacables que versan sobre el contexto internacional al que hacemos referencia más arriba y que forma parte de los álgidos debates actuales. El primero lo constituye la *"Declaración conjunta de la República Popular China y la Federación de Rusia sobre la profundización de la asociación estratégica de colaboración integral en la nueva era con motivo del 75º aniversario del establecimiento de relaciones diplomáticas entre los dos países"*, que anuncia un "Nuevo Orden Internacional", que pretende reemplazar al que se encuentra vigente desde el fin de la Segunda Guerra Mundial. Luego incorporamos el texto completo titulado *"Unclassified Report"*, emitido por las agencias de seguridad de los EE. UU. que trascendió a los medios de comunicación recientemente, y finalmente la entrevista concedida dentro de la: "*Conferencia de Seguridad de Múnich: el Alto Representante Josep Borrell sobre la nueva agenda geopolítica"*, que nos permite conocer la posición europea al respecto.

Finalmente, incorporamos una interesante reseña del último libro publicado por Henry Kissinger, a sus 99 años, titulado *"Liderazgo. Seis estudios sobre estrategia mundial"*, que sin duda será de gran interés para los lectores.

Dr. Juan Fuentes Vera
Editor Responsable


ACADEMIA NACIONAL DE ESTUDIOS POLITICOS Y ESTRATEGICOS
CHILE

ARTÍCULOS

HACIA UNA PROPUESTA DE SEGURIDAD NACIONAL A LA LUZ DE LOS CASOS DE CHILE Y MÉXICO Y EL COMBATE AL CRIMEN ORGANIZADO∞

DIEGO RAMÍREZ SÁNCHEZ•

RESUMEN

En el artículo se realiza una propuesta conceptual de Seguridad Nacional, entendiéndola como una condición conformada por dos dimensiones complementarias: la seguridad exterior y la seguridad interior. Para lograrlo se utilizan como base los casos chileno y mexicano, en tanto el conflicto ancla que se utilizará para problematizar el concepto es el del combate al crimen organizado. El análisis propone que el fenómeno criminal mencionado es capaz de transformarse en una amenaza a la seguridad interior que, al agravarse, amenaza a su vez la seguridad nacional. Al mismo tiempo, asevera que la definición concreta de los conceptos de seguridad adoptada por un país, o la falta de esta, condiciona la respuesta nacional a este tipo de amenazas, así como las instituciones construidas para este fin.

Palabras clave: *Seguridad Nacional; Seguridad Interior; Seguridad Pública; Chile;* México.

TOWARDS A PROPOSAL FOR NATIONAL SECURITY IN LIGHT OF THE CASES OF CHILE AND MEXICO AND THE FIGHT AGAINST ORGANIZED CRIME

ABSTRACT

In the article, a conceptual proposal of National Security is presented, understanding it as a condition shaped by two complementary dimen-

• Licenciado en Historia (PUC), Licenciado en Seguridad y Defensa (ANEPE), diplomado en Estudios Estratégicos (ACAGUE/ IEI-U. Chile), diplomado en Métodos y Técnicas de Análisis en Seguridad Internacional (IEI-U. Chile). Estudiante del Magíster en Seguridad, Defensa y Relaciones Internacionales (ANEPE) y del diploma de experto universitario en Crimen Organizado Transnacional y Seguridad (UNED/IUGM). dramirezs123@gmail.com ORCID: https://orcid.org/0000-0003-0023-6665

∞ Fecha de recepción: 021023 - Fecha de aceptación: 260624.

sions: external security and internal security. To achieve this, the Chilean and Mexican cases are used as a basis, with the anchor conflict being the fight against organized crime. The analysis suggests that the mentioned criminal phenomenon has the potential to evolve into a threat to internal security, which, when exacerbated, in turn threatens national security. Simultaneously, it asserts that the specific definition of security concepts adopted by a country, or the lack thereof, conditions the national response to such threats, as well as the institutions established for this purpose.

Key words: *National Security; Homeland Security; Public Security; Chile; Mexico.*

PARA UMA PROPOSTA DE SEGURANÇA NACIONAL À LUZ DOS CASOS DO CHILE E DO MÉXICO E O COMBATE AO CRIME ORGANIZADO

RESUMO

No artigo é realizada uma proposta conceitual de Segurança Nacional, compreendendo-a como uma condição formada por duas dimensões complementares: a segurança externa e a segurança interna. Para chegar ao objetivo, se utilizam como base os casos chileno e mexicano, enquanto o conflito referência para problematizar o conceito é o do combate ao crime organizado. A análise propõe que o fenômeno criminal mencionado é capaz de se transformar em uma ameaça à segurança interna que, ao se agravar, ameaça por sua vez a segurança nacional. Ao mesmo tempo, o artigo demonstra que a definição concreta dos conceitos de segurança adotados por um país, ou a falta desta, condiciona a resposta nacional a esse tipo de ameaça, bem como as instituições construídas para essa finalidade.

Palavras-chave: *Segurança Nacional; Segurança Interna; Segurança Pública; Chile; México.*

Introducción

En un momento en que Chile vive un proceso de fortalecimiento del crimen organizado a niveles nunca vistos, se vuelve necesario poder definir a qué nos referimos de manera concreta cuando hablamos de seguridad. En este sentido, se ha podido ver cómo el crimen organizado se ha instalado en el país de diversas formas; tanto como mercado ilegal como a través de gérmenes de control territorial. En este sentido, ya se advertía a inicios de 2023, a la luz de las cifras oficiales analizadas hasta 2022 que, a pesar de que Chile se mantiene alejado de los niveles de criminalidad de otros países de la región, sí existían datos preocu-

pantes: Existía un alza en los homicidios, en las incivilidades que involucraban armas, en los homicidios con imputado desconocido y en los secuestros[1].

Si bien los homicidios han mostrado una pequeña disminución el último año, eso no implica necesariamente un quiebre con la tendencia presentada anteriormente[2]. De esta manera, podrían estar generándose gérmenes de lo que se ha denominado "enclaves criminales", los cuales al solidificarse pueden llegar a poner en riesgo la soberanía de los Estados, disputándole no solo el monopolio de la fuerza al Estado, sino también el poder en el territorio[3].

Es en este contexto que Chile no cuenta con definiciones constitucionales ni legales de Seguridad Nacional, así como tampoco de Seguridad Interior. Al mismo tiempo, se mantiene abierta la discusión sobre la pertinencia o no de estos conceptos, lo que se ha visto expresado tanto en la discusión pública, como en las propuestas constitucionales generadas los años 2022[4] y 2023[5]. Así, la respuesta ante las diferentes amenazas a la seguridad no ha contado con una base conceptual que permita entregarles una base sólida, lo que ha impactado en su diseño. El caso de la discusión sobre la protección de la infraestructura crítica, que involucró finalmente una reforma constitucional, y la inclusión de las FF. AA. en tareas tradicionalmente consideradas como de Seguridad Interior, es solo un ejemplo de aquello[6].

Ante esta situación el artículo presentará una revisión de los conceptos de Seguridad Nacional y Seguridad Interior utilizados en la legalidad y en las discusiones en Chile y México. Al mismo tiempo, se dará una primera mirada a las posibles consecuencias que estas definiciones tienen en la construcción de la seguridad, en tanto esto permite apreciar su utilidad práctica en el diseño de políticas y estrategias que permitan definir y combatir amenazas y gestionar riesgos a estas. Se revisará cómo el crimen organizado se puede constituir como una amenaza a la seguridad nacional, a través de la disputa del control territorial y del monopolio de la fuerza, afectando la soberanía nacional. De esta manera una amenaza a la seguridad interior se configuraría en una amenaza a la seguridad nacional; luego se analizarán las definiciones existentes en ambos países en sus distintos instrumentos legales, para continuar con la discusión pública y académica sobre el tema. La última parte del artículo

1 CARVACHO, Pablo y RUFS. 2023. "Series sobre la criminalidad en Chile", Centro de Estudios Justicia & Sociedad, enero 2023. Disponible en: https://justiciaysociedad.uc.cl/seriessobre-la-criminalidad-en-chile/

2 SPD. 2024. Informe Nacional de Víctimas de Homicidios Consumados en Chile, Primer Semestre 2023. Fiscalía-SPD. Disponible en: https://prevenciondehomicidios.cl/wp-content/uploads/2024/01/Informe-Victimas-de-Homicidios-Consumados-al-Primer_Semestre_2023.pdf

3 SULLIVAN, John P. 2023. Crime wars: Operational perspectives on criminal armed groups in Mexico and Brazil. Disponible en: https://international-review.icrc.org/articles/crime-wars-operational-perspectives-923#footnoteref2_j43abzd

4 CONVENCIÓN CONSTITUCIONAL. 2022. "Propuesta Constitución Política de la República de Chile". Disponible en: https://www.chileconvencion.cl/wp-content/uploads/2022/08/Texto-CPR-2022-entregado-al-Pdte-y-publicado-en-la-web-el-4-de-julio.pdf

5 CONSEJO CONSTITUCIONAL. 2023. "Propuesta Constitución Política de la República de Chile" Disponible en: https://www.procesoconstitucional.cl/docs/Propuesta-Nueva-Constitucion.pdf

6 BIBLIOTECA DEL CONGRESO NACIONAL. 2023. Ley 21.542 *Modifica la Carta Fundamental con el objeto de permitir la protección de la infraestructura crítica por parte de las Fuerzas Armadas, en caso de peligro grave o inminente.* Disponible en: https://www.bcn.cl/leychile/navegar?idNorma=1188583

presentará la conclusión, que constará de la propuesta conceptual, así como nuevas líneas de investigación que se puedan derivar de esta.

La elección de los países no ha sido al azar. Si bien ambos casos son distintos, pues el fenómeno de las insurgencias criminales[7] presente en México reviste una mucha mayor gravedad que la amenaza criminal en Chile, la tendencia presente en este último país no lo exime del riesgo de enfrentarlo en el futuro. De esta manera, una revisión de este caso tiene un carácter pedagógico, en tanto nos permite adelantarnos a un posible desarrollo de amenazas a nuestra Seguridad Nacional.

Al mismo tiempo, Chile es un país que adolece de falta de definiciones, a pesar de que en los últimos años se ha dado una discusión pública y académica sobre el particular. Es importante hacer notar que en este país no existe un consenso en torno a la utilización del concepto de Seguridad Nacional, habiendo sectores que niegan su validez conceptual[8], por lo que en vez de definirlo abogan por su eliminación. Por el contrario, otros sectores defienden su vigencia[9] sin que, hasta el día de hoy, alguna de estas posiciones se haya refrendado en determinaciones a nivel legislativo ni constitucional. Debido a esto, los gobiernos tienen espacio para adaptar el concepto en base a sus necesidades cortoplacistas, sin generarse una proyección a nivel de Estado. Sin embargo, la Convención de Naciones Unidas sobre crimen organizado permitiría considerar aspectos que podrían constituir una amenaza a la soberanía nacional de los Estados[10].

Por su parte, México es un país al que su propia crisis de inseguridad, agravada luego de la declaración de "guerra al narcotráfico" por parte del presidente Felipe Calderón el 2006, ha impulsado a llevar adelante discusiones de alto nivel en torno a qué es la seguridad nacional y su relación con la seguridad interior. Asimismo, ha realizado numerosas reformas legislativas e institucionales, expresadas tanto en su ley de seguridad nacional como en las reformas a los organismos policiales federales y a la Guardia Nacional. Así, al contrario de Chile, este es un país en que la discusión no ha estado centrada en la aceptación o no de la seguridad nacional, sino más bien en torno a su contenido y en cómo interactúa con otras seguridades como la seguridad interior y la seguridad pública[11]. En otras palabras, México es un caso que nos permite analizar tanto las discusiones conceptuales como las

7 VOETEN, Teun. 2020. *Mexican drug violence: hybrid warfare, predatory capitalism and the logic of cruelty*. Xlibris.

8 Grupo de Análisis de Fuerzas Armadas y Defensa. 2022. "Reconocimiento a convencionales que trabajaron el tema Fuerzas Armadas y Defensa Nacional". *El* Mostrador. 19 de septiembre de 2022. Disponible en: https://www.elmostrador.cl/noticias/opinion/2022/09/19/reconocimiento-a-convencionales-que-trabajaron-el-tema-fuerzas-armadas-y-defensa-nacional/

9 GRIFFITHS Spielman, John y TORO, Juan Pablo. 2020. *Desafíos para la Seguridad y la Defensa en el Continente Americano, 2020-2030*. Santiago: Athenalab. Disponible en: https://athenalab.org/wp-content/uploads/2020/12/libro_FFAA_athenalab.pdf

10 Naciones Unidas. Oficina contra la Droga y el Delito. Convención de las Naciones Unidas contra la delincuencia organizada transnacional y sus protocolos. Disponible en: https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-s.pdf

11 MOLOEZNIK, Marcos Pablo. 2022. "Seguridad, Defensa e Instrumentos Coercitivos Mexicanos". En: GUERRERO Agripino, Luis Felipe y MOLOEZNIK, Marcos Pablo. *Seguridad y monopolio de la fuerza en México, 2018-2021*. Ciudad de México. Universidad de Guanajuato.

consecuencias prácticas a la hora de combatir amenazas que incluyen al crimen organizado disputando control territorial y monopolio de la fuerza.

Es de vital importancia que se discuta y defina qué se quiere decir cuando se habla de "seguridad nacional" y "seguridad interior". Los retos para los Estados se vuelven cada día más complejos, con amenazas transnacionales que vuelven urgente adoptar medidas del mismo cariz[12]. El problema es que, sin definiciones claras en torno a qué es la seguridad, que sirvan de base para estructurar estas políticas y estrategias sectoriales, se vuelve muy difícil diseñar y evaluar los instrumentos y herramientas de los que se dispone. En este sentido, Emilio Vizarretea nos dice que "…desde la seguridad, debemos establecer claramente qué es lo importante, lo urgente, lo prioritario, lo estratégico. Manteniendo la perspectiva relacional de que los errores de la teoría tienen costos altos en la práctica…"[13]. De esta manera, las definiciones que se manejen y se estipulen en un país, entregan el marco dentro del cual se diseñarán y actuarán las instituciones de seguridad, en los diferentes niveles que se definan. Por el contrario, si no existen estas se abre espacio para un mayor margen de improvisación, así como de confusiones, superposición de funciones y conflictos entre instituciones[14].

Finalmente, a partir de este análisis se buscará realizar un aporte a las discusiones llevadas a cabo en Chile a través de una definición de Seguridad Nacional, así como de su relación con la Seguridad Exterior e Interior, a la luz de la amenaza del crimen organizado. Con tal de realizar esto, el análisis a realizar será cualitativo, revisándose material legislativo, así como trabajos académicos y discusión pública referidos a aquel y al crimen organizado como amenaza a la seguridad nacional.

El crimen organizado como una amenaza a la soberanía

En Chile se define el crimen organizado como "distintas actividades que se llevan a cabo por estructuras organizacionales y que actúan con el propósito de cometer delitos. Las organizaciones criminales pueden ser locales o transnacionales y se pueden entremezclar distintos niveles de organización"[15]. Como se puede apreciar, en primera instancia esta definición no presenta elementos que puedan implicar, *per se*, una posible amenaza a la seguridad nacional, más bien se circunscribe a un problema de seguridad pública. El problema se suscita cuando las organizaciones criminales evolucionan y pasan de ser organizaciones enfocadas exclusivamente en el lucro a través de métodos criminales, a detentar, de facto, el poder en un territorio determinado.

---

12 MEJÍA Rosas, Jorge y WERDAN Torres, Leonardo. Amenazas transnacionales y los roles de los ejércitos. 2018. *Los Ejércitos y el sistema internacional contemporáneo: Nuevas amenazas, tendencias y desafíos*. Escuela Superior de Guerra "General Rafael Reyes Prieto". pp. 47-92. Disponible en: https://docplayer.es/88575953-Los-ejercitos-y-el-sistema-internacional-contemporaneo.html

13 VIZARRETEA Rosales, Emilio. 2013. Estabilidad y Desarrollo Regional para la Seguridad Mexicana. Varios Autores. *La Seguridad Nacional Integral de México*. México D.F: Secretaría de Marina - Armada de México Centro de Estudios Superiores Navales (CESNAV). pp. 61 - 76. p. 83.

14 ORDOÑEZ Martínez, Gustavo. 2021. "La Adopción del Concepto de Seguridad Nacional en México y América latina: Fundamentos, Límites y Perspectivas". *Revista "Política y Estrategia"*, 137. pp. 121-146. p. 123. Disponible en: https://www.politicayestrategia.cl/index.php/rpye/issue/view/37

15 Subsecretaría del Interior. 2022. *Política Nacional contra el Crimen Organizado.* Ministerio del Interior y Seguridad Pública. Disponible en: https://media.elmostrador.cl/2022/12/Poli%CC%81tica-Nacional-contra-el-Crimen-Organizado-del-Gobierno-de-Chile-diciembre2022.pdf. p. 8.

En este sentido John P. Sullivan advierte que es posible que, bajo ciertas condiciones y procesos, actores criminales evolucionen a lo que ha sido denominado insurgencias criminales[16]. Estos generarían enclaves criminales o ciudades asilvestradas (feral cities)[17] en los que, aprovechándose de la debilidad del Estado, y de sus propias capacidades económicas y coercitivas, disputarían la soberanía nacional, llegando a generar incluso espacios de poder dual[18]. De esta forma, organizaciones criminales, sean carteles o bandas criminales, se enfrentan al Estado dando pie a un tipo de insurgencia que no está motivada inicialmente por motivos políticos. Es el fortalecimiento de un actor criminal específico, en un territorio dado, lo que le genera intereses políticos concretos. Así, este se aprovecha de las fisuras que encuentra ante la debilidad de la sociedad y del Estado, pugnando luego por ganar el poder. Pero un enclave criminal puede adoptar diversas dimensiones, variando desde unas cuantas viviendas, hasta un barrio o una ciudad[19]. La cooptación y la corrupción son elementos claves en el proceso por el cual las organizaciones criminales penetran en el Estado, debilitándolo a la vez que se fortalecen, y es un factor incluido en la medición del avance criminal y en el establecimiento de las llamadas "ciudades asilvestradas"[20]. El objetivo de esta insurgencia no sería la toma del poder, sino la de debilitar al Estado, incluso "balcanizándolo", con tal de asegurar su propia autonomía territorial[21].

Para comprender la manera en que estos actores criminales son capaces de disputarle el poder al Estado, aunque sea localmente, es útil adoptar el marco de análisis presentado por David Kilcullen en su obra "Out of the Mountains"[22]. Aquí el autor desarrolla la que denominó como "Teoría del Control Competitivo". Esta indica que los grupos armados no estatales, de cualquier tipo, extraen su fuerza y libertad de acción de su habilidad de movilizar y manipular poblaciones. Lo lograrían a través de un amplio espectro de métodos que variarían desde la persuasión hasta la coerción, creando un marco normativo que generaría en la población un sentimiento de seguridad a través de la previsibilidad y el orden que serían capaces de instituir en un territorio determinado. A esto podríamos agregar que estos grupos armados no estatales son capaces de lograr la instalación de su marco normativo debido a que tienen el poder suficiente para hacerlo.

Para el autor existe una variedad de marcos normativos en pugna, cada uno impulsado por algún actor estatal o no estatal. Mas solo los actores colectivos y armados tienen posibilidad de imponer su marco normativo en un territorio y población determinados, siendo

16 SULLIVAN, John P. 2011. "From Drug Wars to Criminal Insurgency: Mexican Cartels, Criminal Enclaves and Criminal Insurgency in Mexico and Central America. Implications for Global Security". Working Paper No. 9, Fondation Maison des sciences de l'homme. Disponible en: https://shs.hal.science/halshs-00694083/document

17 NORTON, Richard. 2003. "Feral Cities". Naval War College Review 65, N° 4. pp. 97-106, p. 98.

18 SULLIVAN. 2011. Op. Cit. p. 4.

19 Ibíd. pp. 7-8.

20 BUNKER, Robert J. Bunker y SULLIVAN John P. 2011. Integrating feral cities and third phase cartels/ third generation gangs research: the rise of criminal (narco) city networks and BlackFor. *Small Wars & Insurgencies*. 22:5. pp. 764-786.

21 ELKUS, Adam y SULLIVAN, John P. "State of Siege: Mexico's Criminal Insurgency", en: BUNKER, Robert y SULLIVAN, John P. 2012. *Mexico's Criminal Insurgency a Small Wars Journal* – En: *Centro Anthology*. iUniverse, Inc. p. 12.

22 KILCULLEN, David. 2013. *Out of the Mountains, the coming age of the urban guerrilla*. Nueva York: Oxford University Press.

justamente estas las 2 características básicas de aquellos[23]. Así, a través de este proceso, un actor armado, incluyendo uno de carácter criminal, podría no solo obtener el control sobre un territorio, sino a la vez ganar legitimidad ante la población.

Guillermo Valdés Castellanos refuerza esta propuesta al decirnos, desde el contexto del combate al crimen organizado, que es posible apreciar cómo la normatividad existente en una sociedad es fruto de luchas y conflictos entre diversos grupos (ciclo que nunca termina). De la misma forma, existen normatividades paralelas, e incluso opuestas, a las impulsadas por los gobiernos, y que las organizaciones criminales son un ejemplo de actores que basados en su capacidad militar (es decir de coerción), imponen su propia normatividad[24].

Por su parte, Ioan Grillo ha documentado este tipo de fenómenos en su libro "Gangster Warlords" o caudillos criminales[25]. En este describe cómo organizaciones criminales pasaron de ser actores que operaban en mercados ilegales, a insurgencias criminales que controlaban importantes territorios en diversas urbes de países como Brasil, Jamaica, el triángulo norte de Centroamérica y México.

Por último, Esteban Arratia señala que los actores no estatales (en este caso de carácter criminal) afectan el propósito del Estado y tienen implicaciones políticas, ya que se convierten en una competencia a este[26]. Estos podrían ganar legitimidad (los corazones y las mentes) ante la población, a través de la entrega de seguridad y distintos bienes. Para poder contrarrestar esto, el Estado necesitaría fortalecer su presencia territorial y recuperar la lealtad de la población.

De esta manera, podemos apreciar cómo se constituye un marco conceptual que nos permite apreciar el potencial del crimen organizado para establecerse como una amenaza a la seguridad nacional. Hemos visto cómo en determinadas circunstancias de debilidad estatal y societal, un actor armado puede tener la capacidad de instalarse como una competencia hacia el Estado. No solamente es su poder económico el que se lo permite, sino que también su capacidad de coerción y, a la vez de convencimiento a través de la entrega de seguridad, bienes y servicios. Así, se generan enclaves criminales que puedan caer fuera del control estatal, disputándose *de facto* el monopolio de la violencia y la soberanía del Estado. Un problema que pudo entenderse como puramente criminal en un comienzo, se agrava hasta poner en riesgo la seguridad interior del país, y a través de ella, a la seguridad nacional.

Las definiciones legales de seguridad en México y Chile

Con respecto a las definiciones legales que ambos países se han dado, podemos decir que México y Chile contienen diversas referencias legales y constitucionales sobre los conceptos de seguridad nacional e interior, con la diferencia de que en el primer caso existen definiciones explícitas, mientras que en el caso chileno solo existen menciones sin profundización conceptual. En el caso mexicano el concepto se encuentra presente en la

23 Ibíd. p. 132.

24 VALDÉS, Guillermo. 2013. *Historia del Narcotráfico en México* (1a edición ed.). México D.F.: Aguilar. P. 379.

25 GRILLO, Ioan. 2016. *Gangster Warlords: Drug Dollars, Killing Fields and the New Politics of Latin America.* London: Bloomsbury Press.

26 ARRATIA, Esteban. 2016. *Upp's y la pacificación de las favelas en Río 2016 ¿Lecciones para Chile?* En "Anuario de los Cuadernos de Trabajo 2016". CIEE-ANEPE. p. 17.

Constitución Política de los Estados Unidos Mexicanos, en la Ley de Seguridad Nacional de 2005, en la Ley General de Sistema Nacional de Seguridad Pública de 2009 y en la invalidada Ley de Seguridad Interior de 2017. Es importante hacer notar, además, que en la abrogada "Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental" de 2002 también se definía el concepto, lo que generaba complejidades por ser diferente a la utilizada en la Constitución.

La Constitución Política de los Estados Unidos Mexicanos, en su artículo 21 número 9, define el concepto de seguridad pública como una función estatal, mas no se explaya en su posible relación con la seguridad nacional ni interior. Sí señala sus fines, así como las acciones que comprende[27].

A su vez, se mencionan la seguridad nacional e interior en el artículo 89 fracción 6 en tanto facultades y obligaciones del presidente[28], pero a diferencia del caso anterior no se las define. Son mencionadas como una obligación y se las relaciona con las Fuerzas Armadas, no con las policías, y se remite a la ley respectiva para su desarrollo. Con todo, es interesante que se relacione explícitamente la seguridad nacional con la seguridad interior y la defensa exterior de la Federación, como partes de un todo representado en la primera y relacionándolas inequívocamente con las Fuerzas Armadas.

Conforme avanzó el nuevo milenio se fueron desarrollando las definiciones. Así, el 2005 se publica la Ley de Seguridad Nacional, la que dice en su artículo 3° que "Para efectos de esta Ley, por Seguridad Nacional se entienden las acciones destinadas de manera inmediata y directa a mantener la integridad, estabilidad y permanencia del Estado Mexicano…"[29]. En este caso, y a diferencia de las menciones constitucionales, se define una seguridad como acciones y no como una condición a generar ni como función.

Por su parte, en el artículo 2 de la Ley General del Sistema Nacional de Seguridad Pública se desarrolla el concepto de seguridad pública, en tanto función, fines y dimensiones involucradas, pero nuevamente sin relacionarla con los demás niveles de seguridad[30].

Finalmente, en la abrogada Ley de Seguridad Interior se podía encontrar una definición de seguridad interior. En su artículo 2° se la definía como una condición proporcionada por el Estado, que salvaguarda el funcionamiento del gobierno y sus instituciones. También la relacionaba con el desarrollo nacional, la estabilidad constitucional y el Estado de derecho. Incluía los organismos, procedimientos y acciones involucradas, así como la relación entre distintos niveles de gobierno cuando la seguridad nacional estuviera comprometida[31].

Como vemos, el entramado legal y constitucional mexicano presenta varias conceptualizaciones de seguridad, definiendo constitucionalmente la seguridad pública, pero refiriendo la seguridad nacional a su ley específica. Al mismo tiempo, la primera cuenta con una ley que le brinda estructura a través de un sistema nacional, sin existir un sistema análogo para la seguridad nacional. Si bien se intentó definir la seguridad interior, la ley fue

27 Estados Unidos Mexicanos. 1917. Constitución Política de los Estados Unidos Mexicanos. 1917. p. 25.

28 Ibíd. p. 89.

29 Estados Unidos Mexicanos. 2017. Ley de Seguridad Interior. p. 1.

30 Estados Unidos Mexicanos. 2009. Ley General de Sistema Nacional de Seguridad Pública. p. 1.

31 Estados Unidos Mexicanos. 2017. Ley de Seguridad Interior. p.1.

declarada inconstitucional, al entenderse por parte de la Suprema Corte de Justicia que le daba atribuciones que no correspondían a las Fuerzas Armadas.

Como demuestra este esfuerzo legislativo, se ha intentado dar cuerpo legal a las seguridades mencionadas, sobre todo desde comienzos del milenio, cuando durante la alternancia del ejecutivo, el poder del crimen organizado se comenzó a entender como un peligro para la seguridad nacional. Así, surgen las distintas leyes en 2005, 2009 y 2017.

Pero si bien se avanzó en definiciones, no se logró entender ni plasmar la interacción entre los diversos niveles de seguridad definidos, ni tampoco uniformizar las definiciones en tanto condición, derecho y función. El ejemplo más claro es el de la seguridad nacional, a la que se define en tanto acciones. Con todo, se vuelve imprescindible hacer notar que hubo esfuerzos que no implicaron definiciones legislativas. El "Programa para la Seguridad Nacional 2014-2018", del gobierno del presidente Peña Nieto, explicitaba una consideración de esta en tanto función del Estado y con una naturaleza multidimensional[32]. Pero por su propia naturaleza de política de gobierno, no pasó de ser una definición limitada a un partido y período de gobierno específico. Al mismo tiempo, se continuó considerando a los niveles de Seguridad Nacional e Interior como directamente ligados a las Fuerzas Armadas, lo que condicionaría las respuestas que desde el Estado se den ante fenómenos como el crimen organizado.

Por su parte, en Chile el concepto de seguridad nacional aparece numerosas veces en la Constitución Política, sin que se entregue una definición del concepto[33]. Al mismo tiempo, en la Ley Orgánica Constitucional de Carabineros, en su artículo 1°, se hace referencia a la "seguridad pública interior", nuevamente, sin mayor trabajo conceptual. Tampoco hay definiciones en las leyes de Seguridad Interior del Estado ni en la llamada "Ley Antiterrorista", las que se limitan a describir los delitos penados en cada una. Con todo, es interesante realizar una revisión a los diversos libros de la defensa, como el Libro de la Defensa Nacional del 2017 y a la Política de Defensa del 2020, que si bien no son documentos legislativos, sí son importantes en el ordenamiento de la Defensa y trabajan definiciones conceptuales con consecuencias concretas en el quehacer del área.

En el caso de la Constitución Política de la República de Chile, ya en su artículo 1° se menciona la seguridad nacional en tanto deber del Estado, es decir como una función, pero sin mayor definición. El resto de las menciones son en tanto limitante a algún derecho, en el caso de que se la ponga en peligro; como deber ciudadano; como condición que involucra atribuciones del presidente; como rol de las FF. AA. y en el capítulo dedicado al llamado "Consejo de Seguridad Nacional", en el que se especifica su rol asesor, pero sin ningún tipo de definición ni principio rector[34]. Chile, además, no cuenta con ninguna ley de seguridad nacional. Con todo, quizás la mención más importante a este concepto en la Constitución, sea aquella inserta en el artículo 101, el que explicita que las FF. AA. son esenciales para la

32 Presidencia de la República-México. 2014. Programa para la Seguridad Nacional 2014-2018. p. 19. Disponible en: https://www.casede.org/index.php/biblioteca-casede-2-0/seguridad/seguridad-nacional/35-programa-para-la-seguridad-nacional-2014-2018.

33 República de Chile. 1980. Constitución Política de la República de Chile.

34 Ibíd. p. 77.

seguridad nacional[35]. Si bien no se instaura una mención en tanto herramientas exclusivas para lograrla, es decidor que para el caso de las policías, se las circunscriba a otro nivel, sin relacionarlas a la seguridad nacional.

En el caso de la Ley 18.314, que "determina conductas terroristas y fija su penalidad", no se hace ninguna mención a la seguridad, sino que se limita a explicar cuáles serían los delitos que, de acuerdo con ciertas características, serían considerados de tipo terrorista[36].

Por su parte, la "Ley Orgánica Constitucional de Carabineros", en su artículo 1°, nos indica entre las funciones de Carabineros de Chile la de "…mantener el orden público y la seguridad pública interior…"[37]. Se hace referencia a esta función en artículos posteriores, pero en ningún caso se detalle qué implicancias tiene el concepto, ni tampoco existe una ley específica que trate la materia de la denominada "seguridad pública interior", tampoco se la relaciona con la seguridad nacional.

Para finalizar la revisión del cuerpo legal relacionado con las seguridades interior y pública, revisaremos el decreto 890 que Fija el Texto Actualizado y Refundido de la Ley 12.927, sobre Seguridad del Estado. A pesar de lo que su nombre indica, en este decreto no se presenta ninguna definición o noción sobre lo que es en sí misma la seguridad del Estado. Más bien la ley se decanta por enumerar los delitos en contra de la soberanía nacional y en contra de la seguridad interior del Estado, sin tampoco definir esta última[38]. Tampoco existen definiciones sobre seguridad interior, seguridad interior del Estado, ni seguridad nacional en el Código de Justicia Militar[39], ni en el Código Penal[40].

En cuanto a las definiciones manejadas en el sector defensa, revisaremos el Libro de la Defensa Nacional de Chile 2017 y la Política de Defensa Nacional de Chile 2020. En estas publicaciones sí podremos encontrar definiciones específicas, a diferencia de la legislación revisada anteriormente.

En el primer caso se define "seguridad" como una condición a alcanzar, y por ende como el resultado de acciones llevadas adelante con tal de construirla. Al mismo tiempo, se le relaciona directamente con los objetivos e intereses nacionales[41]. Por su parte, se le distingue del concepto de defensa al circunscribir a esta al ámbito de lo militar, y en tanto tal, como un componente esencial pero no único para lograr la seguridad[42].

Ambos casos son interesantes, puesto que en la primera se define el concepto de seguridad en tanto condición, y se la relaciona directamente con un conjunto de actividades que la generarían. Se entiende entonces la condición de seguridad como una condición

35 Ibíd. p. 75.

36 República de Chile. 1984. Ley 18.314 Determina Conductas Terroristas y fija su Penalidad.

37 República de Chile. 1990. Ley 18.961 Ley Orgánica Constitucional de Carabineros. p.1.

38 República de Chile. 1975. Decreto 890 Fija Texto Actualizado de la Ley 12.927, sobre Seguridad del Estado.

39 República de Chile. 1944. Decreto 2.226 Código de Justicia Militar.

40 República de Chile. 1874. Código Penal.

41 Ministerio de Defensa Nacional. 2017. Libro de la Defensa Nacional de Chile. Santiago de Chile: Ministerio de Defensa Nacional. p. 102.

42 Ibíd.

dinámica, que no es estática ni permanente, y que debe ser generada conscientemente a través de acciones especialmente diseñadas para ello. Esto habla de una cierta historicidad del concepto, el que, a pesar de estar relacionado con los objetivos nacionales, también responde a su contexto, se adapta a la par de la sociedad a la que responde, así como a las amenazas y riesgos que enfrenta.

Con todo, es importante hacer notar que el concepto definido en este libro es el de seguridad, y no el de seguridad nacional que es el utilizado en la Constitución, lo que puede interpretarse, a su vez, también como un producto de la historicidad del concepto. Sería la carga histórica de este, más allá del contenido de la definición, la que impulsaría la omisión del apellido "Nacional" en el concepto expuesto, a pesar de su inclusión a nivel constitucional.

En cuanto a su diferencia con el concepto defensa, se considera importante pues permite diferenciarlo de definiciones que relacionaban ambos conceptos, enlazando la seguridad casi exclusivamente con la seguridad exterior. Esta concepción es la que entró en crisis en la inmediata post guerra fría y ha sido fruto de importantes discusiones teóricas[43].

Por otro lado, en el caso de la Política de Defensa 2020 podemos ver que se refiere a un "entorno de seguridad" como condición para lograr un desarrollo integral, para luego definir de manera explícita seguridad nacional como una condición alcanzable, una responsabilidad del Jefe de Estado, y que además comprendería de manera diferenciada la seguridad externa e interna, aunque con límites cada vez más difusos entre ellas[44]. Es interesante la diferenciación explícita que realiza entre ambos componentes, los que *a priori*, pondría en el mismo nivel de importancia. Así, se necesitaría de ambas dimensiones para poder construir la seguridad nacional. Lamentablemente no se profundiza en esta línea, ni se especifica dentro del documento la relación entre estos niveles y las Fuerzas Armadas, así como tampoco el impacto que la difusión de los límites supondría. Lo que sí realiza es una definición de la "condición de seguridad externa", que responde a los parámetros clásicos de esta en torno a independencia, integridad territorial e intereses del país[45].

Para una revisión de discusiones anteriores, es útil remitirnos a la obra de Claudia Fuentes[46], en donde se puede apreciar cómo, en los Libros de la Defensa precedentes (1997 y 2002), se encuentra una contradicción. Por un lado, se integra como dimensión de la seguridad nacional a la seguridad interior, pero por otro se habla de dos ámbitos de cuyas acciones dependería la seguridad: el desarrollo y la defensa[47], ¿dónde entraría entonces la seguridad interior? Para el 2002 se profundizó en la relación entre estos dos ámbitos, en el diseño de una política de seguridad nacional y en los límites que el Estado tiene debido a la

43 GRIFFITHS Spielman, John. 2011. *Teoría de la Seguridad y Defensa en el Continente Americano, Análisis de los casos de EE.UU. de América, Perú y Chile*. Santiago: Ril Editores–USACH.

44 Ministerio de Defensa Nacional. 2021. Política de Defensa Nacional de Chile 2020. Santiago de Chile: Ministerio de Defensa Nacional. p. 11.

45 Ibíd.

46 FUENTES, Claudia. 2005. "Seguridad Humana y Seguridad Nacional: Relación Conceptual y Práctica". Colección de Investigaciones Anepe, N°4.

47 Ibíd. p. 23.

centralidad del bien común y el servicio hacia la persona humana. No se profundiza en el rol de la seguridad interior, que *de facto* queda señalada en un lugar de menor perfil.

De esta manera, la definición de seguridad nacional aquí expuesta es la única referencia al concepto presente hoy en día. Como hemos dicho, a diferencia de México, Chile no cuenta con una ley específica de seguridad nacional, y a nivel constitucional no define ninguna acepción de seguridad.

Una primera comparación entre ambos cuerpos conceptuales nos lleva a señalar que el caso mexicano tiene una mayor cantidad de definiciones a nivel legal, tanto en la Constitución como en leyes. Hubo un intento por explicitar una definición de seguridad interior, pero fracasó por las implicancias prácticas que conllevaba la propuesta en cuanto a DD. HH. y la participación de las FF. AA. en tareas de seguridad interior[48]. De haber prosperado México hubiera tenido definiciones formales en todos los niveles de seguridad.

Pero a pesar de tener definiciones y leyes, es posible ver que no existe un desarrollo en torno a cómo los distintos niveles de seguridad interactúan y relacionan entre sí. Por ejemplo, qué indica cuando un problema de seguridad interior se agrava y se convierte en un problema de seguridad nacional, así como qué significaría esta situación para las instituciones que debieran hacerse cargo. Es importante hacer notar que en la misma Constitución, cuando se habla de seguridad nacional y seguridad interior, se explicita que el Presidente dispone de las FF. AA. para ambas, sin hacerse alusión alguna a algún cuerpo policial de nivel federal.

En el caso chileno la situación es la opuesta. No tiene definiciones concretas de ningún nivel de seguridad en instrumentos legislativos, sino que solamente al nivel de los instrumentos de defensa, tales como el Libro de la Defensa y la Política de Defensa. Una consecuencia de esto es que no existen claridades sobre qué problema, riesgo o amenaza corresponde a cada nivel de seguridad, así como una laguna conceptual al momento de intentar explicitar la relación entre los distintos niveles, al generar políticas y estrategias sectoriales, así como para diseñar o reformar las instituciones encargadas de actuar en cada nivel.

Si bien ambos países han desarrollado sus instrumentos conceptuales en el área de la seguridad, discusión que en México comenzó en la década de 1980[49] pero que se aceleró desde la alternancia política de los primeros 2000, ninguno de los dos países ha logrado tener un desarrollo conceptual explícito a nivel legislativo, que comprenda definiciones claras y que entiendan las seguridades tratadas en tanto condición, función y derecho, así como las relaciones entre los distintos niveles especificados. Esto es aún más patente en el caso chileno, el que solo tiene un trabajo conceptual importante en los instrumentos dedicados a la defensa nacional. De esta manera se genera, aunque sea de manera implícita, una

48 ALCÁNTARA, Suzzete y ARVIZU, Juan. 2019. Ley de Seguridad Interior de EPN es desechada. El Universal. 18 de noviembre de 2019. Disponible en: https://www.eluniversal.com.mx/nacion/ley-de-seguridad-interior-de-epn-es-desechada/

49 MACIEL-PADILLA, Agustín. 2020. El reto de la agenda de defensa de México: la ausencia de un enfoque integral de seguridad nacional. En: GRIFFITHS Spielman, John y TORO, Juan Pablo. 2020. *Desafíos para la Seguridad y la Defensa en el Continente Americano, 2020-2030*. Santiago: Athenalab. pp. 81-103. p. 81.

sobredimensión del sector defensa ante la seguridad nacional, lo que, como vimos, se produce desde la misma Constitución Política de la República.

Sin lugar a duda esto se vuelve un problema a la luz del enfrentamiento al crimen organizado. No existe una claridad conceptual que permita medir fehacientemente el grado de amenaza para reconocer cuándo un problema de seguridad interior pasa a involucrar la seguridad nacional. Tampoco se enfoca el problema desde una perspectiva de sistema, con una arquitectura de seguridad nacional que coordine los subsistemas de seguridad exterior e interior, construyendo interagencialmente la seguridad nacional. Se dificulta, en el fondo, saber cuándo el instrumento a utilizar por el Estado deben ser las Fuerzas Armadas en vez de las policías, si es que en algún momento lo deben hacer, ni tampoco se consideran fuerzas intermedias que se hagan cargo de la seguridad interior de manera diferenciada de la seguridad pública.

¿En base a qué conceptualización de seguridad el Estado podrá leer el surgimiento de gérmenes de enclaves criminales en su interior, o si quienes los levantan son grupos criminales, transnacionales o no, pueden impactar nuestra soberanía nacional? Y si lo hacen, ¿deben ser necesariamente las Fuerzas Armadas quienes se deban hacer cargo?

Intentaremos enriquecer estas cuestiones revisando bibliografía especializada de ambos países.

Las discusiones conceptuales

En ambos países ha habido discusiones, aunque con diferencias derivadas de sus contextos. En México estas han girado en torno a definiciones concretas y sus consecuencias en el contexto al combate al crimen organizado. Mientras en Chile la discusión también ha incluido su pertinencia o no, dejando la cuestión del contenido a veces en segundo plano. Esta es una problemática con consecuencias concretas, como señala Gustavo Ordoñez para el caso de las fuerzas armadas y policiales mexicanas[50].

Así, en México, Marcos Pablo Moloeznik define seguridad en tanto derecho fundamental, como una función privativa del Estado y como condición que el Estado debe asegurar[51], y es en el contexto de estas tres características que se despliegan las distintas definiciones de seguridad utilizadas. Esto, pues existe un concepto de seguridad general "sin adjetivos", cuyo significado no es único, y que es más específico dependiendo de qué adjetivo se le aplique[52]. De esta manera, si bien existe la seguridad, esta se despliega en diversas dimensiones, cada una con su especificidad. El foco estará en las dimensiones "Nacional" e "Interior", que son las que, se postula, se debieran definir y estructurar coherentemente para un mejor sustento en las decisiones estratégicas y políticas del Estado.

50 ORDOÑEZ. Op. Cit. pp. 124; 138.

51 MOLOEZNIK. 2022. Op. Cit. pp. 27 y 30.

52 MARTÍ DE GIDÍ, Luz del Carmen; 2006. La seguridad nacional y el acceso a la información pública en México. Xalapa: s.n. *Letras Jurídicas*, págs. 219-245. pp. 219-220. Disponible en: https://cdigital.uv.mx/bitstream/handle/1944/51453/MartideGidiLuz.pdf?sequence=1

Ya el año 2004 Moloeznik discutía la relación entre seguridad como concepto y los instrumentos coercitivos en México[53]. Aun antes de la aprobación de la Ley de Seguridad Nacional, el autor nos indicaba que el Estado cuenta con instituciones coercitivas para sancionar a quienes violen el marco normativo del país, y que este uso de la fuerza institucional se debe dosificar. Su tesis en ese entonces era la existencia de tres niveles de seguridad, cada una con un determinado instrumento coercitivo. Estos niveles de seguridad tendrían entre sí una relación de tipo jerárquica, con la seguridad nacional en el nivel superior, la seguridad interior en el medio y en la base la seguridad pública.

El autor nos indica que la seguridad nacional estaría relacionada con los intereses vitales de la Nación; es decir, aquellos trascendentes y permanentes como la supervivencia del Estado-Nación. También se relaciona este nivel con las FF. AA., que serían el "argumento final del Estado-Nación"[54], y finalmente con la delincuencia organizada por estar calificada como una amenaza a la seguridad nacional mexicana.

Así, el 2004 se define la seguridad nacional como aquella vinculada con la supervivencia del Estado-Nación, cuya herramienta primordial serían las FF. AA., y que integraría a la delincuencia organizada como una amenaza directa. Tal como se ha expresado, generalmente, en los cuerpos legales revisados anteriormente.

En cuanto a la Seguridad Interior, reafirma la laguna jurídica existente (y que se mantiene hasta el día de hoy), pero a través de la doctrina del Comité Internacional de la Cruz Roja, que la asume como aquella que involucra violencia y disturbios menores que sobrepasen a las fuerzas policiales, en una "zona gris" entre el conflicto armado y la paz[55]. Esta dimensión estaría relacionada con las "Fuerzas de Seguridad" o "Fuerzas Intermedias", o policías con estatuto y capacidades militares capaces de garantizar la estabilidad, la seguridad interior y la paz social[56]. De esta manera, y considerando lo expuesto respecto a este nivel en el primer apartado, el autor nos dice que "…se identifica a la seguridad interior como una vertiente de la seguridad nacional; a la sazón, componente de la seguridad nacional…"[57]. De esta manera, existe un vacío conceptual que traspasa fronteras y que afecta incluso las definiciones en torno a violencia interna que maneja la Cruz Roja. Este organismo tuvo que modificar, debido a la falta de consenso internacional, la expresión "disturbios y tensiones interiores" por la de "otras situaciones de violencia", más indefinida y sin referencia al ámbito interior[58]. En 2012, profundiza en torno al riesgo de la militarización de la "seguridad ciudadana", la que no define y que tampoco está en la legislación mexicana revisada, pero que es asimilable a la seguridad pública. Así, afirma que los integrantes de

53 MOLOEZNIK, Marcos Pablo. 2004. Seguridad y uso de la fuerza en el Estado contemporáneo (una interpretación mexicana sobre los instrumentos coercitivos estatales). 6. *Revista del CESLA.* Pp. 29-36. Disponible en: https://www.revistadelcesla.com/index.php/revistadelcesla/article/view/275/271

54 Ibíd. p. 31.

55 Ibíd. p. 32.

56 Ibíd.

57 MOLOEZNIK, Marcos Pablo y SUÁREZ DE GARAY, María. 2012. El proceso de militarización de la seguridad pública en México (2006-2010). *Frontera Norte*. 24 (48). 121-144. p. 140. Disponible en: https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0187-73722012000200005

58 MOLOEZNIK, Marcos Pablo. 2018b. Presentación: Hacia una interpretación del proceso de militarización de la seguridad pública en América Latina. Contextualizaciones Latinoamericanas. 2 (19). 1-22. p. 2. Disponible en: http://contexlatin.cucsh.udg.mx/index.php/CL/article/view/7286/6432

las FF. AA. no están preparados para misiones policiales o parapoliciales[59], y que el sentido de hacer la guerra es distinto al de hacer cumplir la ley. En el primero se busca eliminar al enemigo, y en la segunda preservar la vida para que actúe la justicia. Así el sentido de la acción es diferente pues se actúa en distintos niveles de seguridad. Queda de manifiesto, de esta manera, el vacío en la intersección entre seguridad nacional e interior, así como la confusión existente con la seguridad ciudadana, impactando a las FF. AA. ya que, si estas no están preparadas para hacerse cargo de esta última, ¿lo están para hacerse cargo de la seguridad interior como indica la legislación?

De esta manera es importante entender que, según lo presentado hasta ahora, no es un hecho banal el que existan diferentes definiciones de niveles de seguridad. Estas definiciones implican también lógicas de construcción distintas, así como herramientas institucionales diferentes, aunque complementarias. Así, el uso de un instrumento coercitivo diseñado para actuar ante situaciones que afecten un nivel específico de la seguridad, en otro, implica el reconocimiento del fracaso de la institución originalmente encargada de ese nivel, como en el caso de la militarización[60]. Al mismo tiempo, no tener estas claridades dificulta el diseño de respuestas a amenazas que, teniendo consecuencias internas, son de naturaleza internacional o transnacional, por lo que, al momento de ser superadas las fuerzas policiales, y quizás al no contar con fuerzas intermedias, se puede legitimar a las fuerzas armadas en tareas de orden interior y/o pública[61].

Un ejemplo de las consecuencias institucionales concretas que tienen las definiciones de seguridad es el caso de la Secretaría de Marina. En el caso mexicano las definiciones utilizadas han generado cambios organizativos, operativos y de equipamiento[62], como en las capacidades de guardacostas y en las fuerzas de infantería de marina[63]. Así, las confusiones conceptuales impactan en la desnaturalización de las FF. AA.

Por otro lado, Agustín Maciel-Padilla hace un aporte a la discusión en su artículo "El reto de la agenda de defensa de México: La ausencia de un enfoque integral de Seguridad Nacional"[64]. En este instala, en concordancia con nuestros autores anteriores, el problema de la confusión conceptual entre los distintos niveles de seguridad, uniéndolo directamente a un impacto negativo en el diseño de políticas públicas[65]. Además, realiza una crítica a la falta de discusión en torno a la temática, que en México se habría iniciado en la década de

59 PONTÓN Cevallos, J. 2014. La militarización de la seguridad ciudadana: una tendencia regional. Entrevista con Marcos Pablo Moloeznik Gruer. URVIO. *Revista Latinoamericana De Estudios De Seguridad*, (12). 143-146. Disponible en: https://www.redalyc.org/pdf/5526/552656545011.pdf

60 Ibíd.

61 SOLÍS Minor, Martha Patricia. 2018. El proceso de militarización de la seguridad pública en México como resultado de la reconfiguración de la política de defensa estadounidense y el combate a las amenazas emergentes en América Latina. *Contextualizaciones Latinoamericanas*. 2 (19). p. 3. Disponible en: http://contexlatin.cucsh.udg.mx/index.php/CL/article/view/7319/6438

62 ORDOÑEZ. Op. Cit. pp. 138-139.

63 MOLOEZNIK, Marcos Pablo. 2018a. Infantería de Marina en América Latina: pasado, presente y futuro, *Revista del Centro de Estudios Superiores Navales*, abril–junio, 39 (2). pp. 11-46. Disponible en: http://repositorio.uninav.edu.mx/xmlui/handle/123456789/486

64 MACIEL-PADILLA. Loc. Cit.

65 Ibíd. pp. 82-83.

los 80 ante el asesinato del agente de la DEA "Kiki" Camarena[66] por presiones de EE. UU. y no a partir de una reflexión nacional. Estas situaciones habrían generado ciertas distorsiones, como que la legislación mezclaría conceptos (como vimos en el caso de su Constitución), así como la relación que se ha generado entre el narcotráfico y su violencia con la militarización de la seguridad pública[67]. Punto aparte al hecho de que la presencia de una agencia extranjera en un país, como el caso de la DEA en México, puede ser por sí mismo un tema complejo en términos de seguridad nacional[68].

Otro elemento a relevar es que, para Maciel-Padilla, las Fuerzas Armadas están íntimamente relacionadas con la Seguridad Nacional, en tanto serían su instrumento por excelencia[69]. De hecho, afirma que la calificación del narcotráfico como amenaza a la seguridad nacional justifica teóricamente la presencia militar[70], relacionándolas explícitamente. Así, a pesar de que se intenta ampliar el concepto más allá de aquellas definiciones herederas de la guerra fría, se continúa haciendo una relación entre este con la función militar encargada de la Defensa, es decir, de la Seguridad Exterior del Estado (más allá de que en México, puntualmente, también se las relacione con la Seguridad Interior).

Por último, es interesante el contrapunto que el autor realiza en torno al concepto de seguridad humana, en tanto esta centraría la seguridad en el individuo dejando de lado al Estado en una concepción multidimensional de esta. Para él esto sería incorrecto, pues el Estado seguiría siendo el actor dominante del sistema internacional, y las fuerzas armadas tendrían un rol en éste[71]. Así, si bien estamos de acuerdo con esto, es notoria la ausencia de la Seguridad Interior y su relación con el Estado, así como con su rol en construir el bienestar en contraposición con la concepción de seguridad humana criticada.

Pero la identificación de las fuerzas armadas con la Seguridad Nacional, en tanto su herramienta predilecta, no es algo exclusivo de México. En el mencionado estudio de Fuentes se da cuenta cómo hasta avanzada la transición democrática en Chile, se mantenía la identificación de la seguridad nacional con la función defensa[72], a pesar de que diversas voces daban por superada la concepción clásica de esta ya en 2008[73], incluyendo sus dos dimensiones de seguridad pública y de defensa nacional.

En cuanto a definiciones de Seguridad Nacional, encontramos una en el libro "Conceptos fundamentales de inteligencia", en el que nuevamente Moloeznik nos presenta una

66 Sobre el caso Camarena, revisar: PÉREZ Ricart, Carlos. 2022. Cien años de espías y drogas, la historia de los agentes antinarcóticos de Estados Unidos en México. Debate.

67 MACIEL-PADILLA. Op. Cit. pp. 82-83.

68 PÉREZ Ricart. Loc. Cit.

69 MACIEL-PADILLA. Op. Cit. pp. 83-84.

70 Ibíd. p. 98.

71 Ibíd. p. 90.

72 FUENTES, Claudia. Loc.Cit.

73 MOLINA, Carlos. 2008. La relación cívico-militar y su incidencia en las políticas de seguridad nacional: la experiencia chilena. *Revista Política y Estrategia N° 110.* ANEPE. pp. 15-16. Disponible en: https://www.politicayestrategia.cl/index.php/rpye/issue/view/9/133

revisión sobre el particular[74]. En esta ocasión se hace hincapié en la falta de consenso internacional en torno a una definición concreta y específica del concepto. Mas, se la relaciona a la integridad, estabilidad y permanencia del Estado, incluyendo sus intereses económicos y políticos vitales; en fin, se presenta un concepto Estado-céntrico, relacionado con los intereses vitales, y por ende permanentes, de la Nación. Por todo esto pertenecería al campo de la conducción político-estratégica del país y al máximo nivel de conducción estatal[75].

Un aspecto interesante de esta propuesta es que plantea una serie de retos y perspectivas: su relación con el contexto político, y por ende su carácter evolutivo e histórico; su fuerte rol en cuanto permite maximizar el poder en la política interna de un país; y su relación con el Estado en tanto orientador de conflictos sociales, instrumento de gobernabilidad y gobernanza, y garante de la seguridad[76].

Desde otro ángulo, María Cristina Rosas nos ilumina con respecto a la importancia de que la seguridad nacional sea una política de Estado y no de Gobierno como estaría ocurriendo en México[77]. Esto redundaría en cambios drásticos a nivel de definiciones, incluso entre distintos períodos de gobierno o entre reparticiones gubernamentales[78], lo que tendría impactos directos en las políticas públicas y estrategias impulsadas. La autora también nos indica que esta no estaría relacionada únicamente con las Fuerzas Armadas, flexibilizando las posiciones de otros autores. Sería una tarea de toda la sociedad, aunque continúa siendo un concepto cargado por la historia[79].

Aquí podemos ver dos elementos interesantes e interrelacionados: por un lado, el entender la seguridad nacional como una tarea del país, y no de ciertos cuerpos profesionales armados (policiales o militares). Esta postura se diferencia claramente de quienes relacionan exclusivamente la seguridad nacional con las fuerzas armadas; y, por otro lado, el fuerte peso negativo que en ciertos sectores tiene el concepto por temas históricos. Esta última situación podría ser enfrentada, entre otras medidas, a través de una definición adecuada que impida la repetición de ese tipo de hechos.

Otro autor que reconoce el carácter de condición de la seguridad nacional es Rubén Guzmán Sánchez, quien la comenta como "…un proyecto futuro a conseguir, o una realidad de facto a mantener (…) y ampliar"[80]. Guzmán también la diferencia con respecto de la seguridad pública, criticando su militarización y el empleo de las fuerzas armadas en su construcción ante la amenaza de los grupos de delincuencia organizada[81].

---

74 MOLOEZNIK, Marcos Pablo. 2016. Seguridad Nacional. Díaz Fernández, A. M. *Conceptos Fundamentales de Inteligencia*. (343-350). Valencia: Editorial Tirant Lo Blanch – Centro Nacional de Inteligencia de España.

75 Ibíd. pp. 343-345.

76 Ibíd. p. 348.

77 ROSAS, María Cristina. 2013. ¿Seguridad Nacional de Estado o de Gobierno? En: ROSAS, María Cristina. *Repensando la Seguridad Nacional de México.* Centro de Estudios Navales (CESNAV). P. 2.

78 Ibíd. p 3.

79 Ibíd. pp. 5-6.

80 GUZMÁN Sánchez, Rubén. 2013. La Seguridad Pública bajo la Seguridad Nacional: el eslabón roto de lo local y la desconexión con la Seguridad Ciudadana. En: ROSAS, María Cristina: *Repensando la Seguridad Nacional de México.* Centro de Estudios Navales (CESNAV).

81 Ibíd. pp. 66-67.

Con respecto a las discusiones llevadas adelante en Chile, empezaremos constatando que la no definición del concepto en la Constitución no es un hecho fortuito. Ya en 1985 Jaime Guzmán, uno de los principales inspiradores de la Constitución vigente, escribía que "… intentarlo [dar una definición exacta] en tal carácter, arriesga empequeñecer sus alcances, peligro común a muchas definiciones de los valores más ricos de la convivencia social"[82], por lo que entendemos que el objetivo de la indefinición conceptual apuntó a entregarle la mayor amplitud posible sin especificar límites ni márgenes.

Como una respuesta a este planteamiento es que se levanta la posición defendida por Augusto Varas, integrante del Grupo de Análisis de Defensa y Fuerzas Armadas (GADFA), quien relaciona seguridad nacional con la denominada "doctrina de seguridad nacional", pero además lo califica como un "significante vacío" que ha implicado una expansión del rol de las FF. AA. en la sociedad chilena[83], proponiendo su desaparición. Esta desaparición conceptual debiera, además, involucrar la utilización del concepto de defensa nacional para definir su principal tarea, eliminando a su vez el actual Consejo de Seguridad Nacional (COSENA), reemplazándolo por un Consejo Superior de la Defensa Nacional[84]. A nuestro juicio esto constituye una demostración de que, a pesar de la posición crítica con respecto a las conceptualizaciones marcadas por la guerra fría, hay sectores que continúan viendo la seguridad nacional como un tema relacionado con la seguridad exterior y la defensa nacional, y sin una relación con la seguridad interior. No existiría un concepto o nivel de seguridad que definiera la seguridad del país como un todo.

Por el contrario, Ernesto Ferrada constata el mismo vacío conceptual, pero impulsa su definición. En su artículo verifica la falta de definición en torno a la seguridad nacional a pesar de ser este un término utilizado de manera profusa en nuestra legislación[85], sin que se la defina en parte alguna. También revisa las diversas definiciones en nuestra región, en Europa y en el derecho internacional, constando que no siempre existe y que, si lo hace, varía de país en país, por lo que reafirma su carácter evolutivo, histórico y contextual. Esto es reafirmado por Ángel Sarmiento cuando nos dice que la seguridad nacional "…no puede ser vista como un concepto inamovible, inflexible, estático o solo como un referente jurídico"[86] y que por ende "…debe adecuarse al entorno contextual de México, con la finalidad de ser compatible y competitivo frente a las nuevas condiciones…"[87]. Por último, poniendo de ejemplo la reunión del COSENA del 7 de noviembre del 2019, Ferrada nos expone que la definición del concepto es necesaria para dar mayor certeza jurídica y para poder

82 GUZMÁN Errázuriz, J. (2016). "Seguridad nacional en la Constitución de 1980". *Revista De Derecho Público*, (37/38), Págs. 45–65- P. 49. Disponible en: https://revistaderechopublico.uchile.cl/index.php/RDPU/article/view/43698

83 VARAS, Augusto. 2020. "Seguridad Nacional: Un significante vacío". *Política, Revista de ciencia política*. 58 (1). pp. 29-56. Disponible en: https://revistapolitica.uchile.cl/index.php/RP/article/view/61561/65343

84 Ibíd. p. 53.

85 FERRADA, E. (2020). La Seguridad Nacional: ¿es necesaria su definición positiva en el derecho nacional? *Escenarios Actuales,* 25(2), 29-48. pp. 31-34. Disponible en: https://www.ejercito.cl/descargas/desktop/NDE4

86 SARMIENTO Beltrán, Ángel Enrique. 2013. Prólogo, La Seguridad Nacional Integral de México: Diagnósticos y Propuestas. Varios Autores. *La Seguridad Nacional Integral de México. Diagnósticos y Propuestas.* Centro de Estudios Superiores Navales (CESNAV-SEMAR) – Universidad del Ejército y Fuerza Aérea (UEFA-SEDENA), México D.F. P. vii.

87 Ibíd.

invocarla en las instancias definidas para ello en la legislación[88]. Es decir, concordando con Maciel-Padilla, se pone de manifiesto el impacto práctico y concreto de su indefinición para el quehacer político y estratégico del Estado.

En la misma línea, Fuentes Vera señala los beneficios que el diseño de estrategias de seguridad tiene para un país, permitiéndole adoptar una mirada de conjunto acerca de los peligros que identifica[89]. Al estar centrada en construir una seguridad de Estado, podrá entregar una orientación general a políticas sectoriales[90]. Pero, justamente debido a los beneficios que una estrategia de este tipo podría tener, y para clarificar además los objetivos a lograr en seguridad y como país, es necesario entregarle una base sobre la cual diseñarla. El no contar con definiciones consensuadas atenta en contra de este tipo de iniciativas.

Para Arancibia Clavel la Constitución de 1980 le plantea dos misiones a las FF. AA. para coadyuvar y permitir el desarrollo nacional, siendo una la de ser esenciales para la seguridad nacional[91]. El que sería el punto de partida de la discusión sobre seguridad nacional y el rol de las FF. AA. Pero esta visión se complementaria, aunque no a nivel constitucional, diferenciándose la seguridad exterior de la seguridad interior, pero nuevamente siempre bajo el marco constitucional dicho. Las policías se relacionarían con la seguridad pública interior, no con la seguridad nacional. Es más, para el autor, "la seguridad y la defensa de la Nación constituyen sin lugar a duda la esencia de las FF. AA." pero dentro de un marco histórico que determina su connotación[92]. Nuevamente se manifiesta la historicidad del concepto, así como se manifiesta una comprensión de la seguridad nacional que pugna por complejizarse, pero que en última instancia continúa siendo definida, en su contorno, por la definición constitucional vigente.

Por su parte, John Griffiths nos hace una propuesta conceptual desde una óptica diferente, en la que relaciona (y diferencia) la seguridad nacional del desarrollo nacional. Así, resalta la importancia de definir la primera para evitar que se pueda considerar todo problema como uno de seguridad, proponiendo una definición más acotada[93] que la defendida, por ejemplo, por Mladen Yopo. Este último autor, si bien la considera como una condición, también la reconoce como un concepto multifuncional y multidimensional, poniendo en duda así las consideraciones clásicas de la seguridad nacional, pero ampliando su enfoque[94].

88 Ibíd. p. 47.

89 FUENTES, Juan. 2012. Hacia una política de Seguridad Nacional: elementos para la discusión. En *Revista Política y Estrategia*. ANEPE. 119. P, 92.

90 Ibíd. p. 126.

91 ARANCIBIA, Daniel. 2020. "Relevancia Constitucional de las FF.AA.: Una Visión Actualizada". En *Anuario de Cuadernos de Trabajo 2020*. CIEE-ANEPE. pp. 62-82. p. 63. Disponible en: https://anepe.cl/wp-content/uploads/2021/05/Anuario-Cuadernos-de-Trabajo-2020.pdf

92 Ibíd. p. 80.

93 GRIFFITHS. 2011. Op. Cit. pp. 9-10.

94 YOPO, Mladen. 2019. "Estrategia de Seguridad: Una Agenda con los ciudadanos". En: *Antecedentes para el Debate Acerca de una Estrategia de Seguridad Nacional, N° 45.* ANEPE. pp. 15-56. pp. 15-17. Disponible en: file:///C:/Users/Irojas/Downloads/LIBRO-ANEPE-45-1.pdf

Grifitths, por su parte, define las amenazas relacionándolas directamente con la seguridad y diferenciándolas entre nacionales, transnacionales y externas[95], pero considerando como amenazas solamente a "…los fenómenos de expresión violenta; mientras que a todos aquellos que generan condiciones de inseguridad, como riesgos estructurales"[96].

Finalmente, se entrega una definición de seguridad consistente en reconocerla como una condición que, junto al desarrollo nacional, permitiría lograr el bien común nacional circunscribiéndola, al mismo tiempo, a los fenómenos violentos e intencionales, y con un ámbito objetivo y otro subjetivo[97].

Es interesante constatar que reafirma la seguridad como una condición a lograr, su carácter no absoluto (por lo que es una tarea permanente e histórica), e innova al relacionar la seguridad con amenazas intencionales militares y no militares; es decir, fenómenos violentos.

Esta reflexión es profundizada por el mismo autor junto a Marcelo Masalleras en un documento de trabajo denominado "La Seguridad del Estado en Chile", realizado a través del centro de pensamiento "Athenalab". En este unen la definición de seguridad presentada por Griffiths con la construcción de una arquitectura de seguridad nacional como herramienta del Estado en un escenario internacional volátil, incierto y ambiguo[98]. Además, responde explícitamente a las posiciones que se oponen a la utilización del concepto, y de paso, a los intentos por lograr una definición más exacta de este[99].

Uno de los elementos novedosos de este documento es que hace una revisión de la vigencia del concepto a nivel internacional, concluyendo que está vigente a nivel académico y en cuanto política pública[100], aunque como vimos no exista un consenso internacional ni regional en cuanto a su significado, y a su carácter ambiguo en tanto responde a decisiones políticas en contextos determinados[101].

Conclusiones

A partir de lo revisado, se aprecia que en la actualidad no existe consenso en una definición de seguridad nacional, ni tampoco en cuanto a la seguridad interior. De todas maneras, la mayoría de las posiciones coinciden en comprenderla en tanto condición, así como en reconocer como parte integrante de esta a la seguridad exterior e interior. Lamentablemente, de esta coincidencia no se desprende una certeza en cuanto al rol de las fuerzas armadas, ni de las instituciones de seguridad interior. Continúa existiendo una inercia que le otorga un papel privilegiado a las fuerzas armadas en la construcción de la seguridad nacional, tal como implícitamente hace la Constitución de Chile, y explícitamente su símil mexicano.

95 Ibíd. p. 558.

96 Ibíd. p. 560.

97 Ibíd. pp. 584-585.

98 GRIFFITHS, John y MASALLERAS, Marcelo. 2022. La Seguridad del Estado en Chile. Athenalab. P. 7. Disponible en: https://athenalab.org/documento-de-trabajo-no18-la-seguridad-del-estado-de-chile/

99 Ibíd.

100 Ibíd. pp. 11 y 18.

101 Ibíd. p. 8.

De esta manera, se pasa de una discusión compleja, a un marco legal poco desarrollado, en el que no se ha logrado plasmar los últimos debates. En ninguno de los dos casos existen definiciones en las líneas revisadas, ni por ende, estrategias, políticas y estructurales institucionales basadas en ellas. El impacto que esto ha tenido en el combate al crimen organizado es evidente, con procesos de militarización de la seguridad pública, y de policialización de fuerzas militares. Hoy no es posible avanzar de manera ordenada en la construcción política e institucional sectorial, ni tampoco leer claramente, a la luz de la seguridad nacional, amenazas como las insurgencias criminales ni el surgimiento de lugares asilvestrados, en donde el crimen dispute la soberanía nacional. Se debe, así, complejizar ya no solo la discusión, sino los marcos jurídicos que rigen la construcción de la seguridad nacional, dotándolos del necesario consenso nacional que les de legitimidad y proyección.

Pero para esto se necesita una propuesta concreta, y retomando diversas posiciones analizadas, se opta por proponer un concepto de seguridad nacional que se comprenda a la vez como función estatal, como derecho y como condición a lograr. Para esto, además, se considera que la seguridad nacional se relaciona fundamentalmente con aquellos fenómenos violentos que afectan la capacidad del Estado y de la sociedad para poder perseguir sus objetivos comunes. Así, esta se conformaría por dos dimensiones complementarias, la seguridad exterior, a cuyo cargo se encontrarían primordialmente la función Defensa y la diplomacia; y la seguridad interior, a cargo de las instituciones de seguridad interior y justicia.

Para efectos de su utilidad, y para evitar la dispersión conceptual, así como la militarización de los más diversos ámbitos, no se amplía el concepto de seguridad a temáticas como la seguridad alimentaria, medioambiental, o de otro tipo. Las tareas de estos ámbitos se consideran parte del desarrollo nacional.

Entendida de esta manera, se vuelve plausible comprender que amenazas a la seguridad interior (tales como el crimen), puedan escalar a ser una amenaza a la seguridad nacional al afectar su soberanía interior. No obstante, esto no implicaría que las fuerzas armadas debieran hacerse necesariamente cargo, pues son las instituciones encargadas de la seguridad interior las que deben hacerlo. Se vuelve necesario, por lo tanto, desarrollar estas instituciones, al mismo tiempo que permitir la coordinación de los sistemas de seguridad exterior e interior, así como su trabajo en común. Solo la complementariedad entre ambas dimensiones permitirá que se logre obtener una condición de seguridad nacional.

Queda pendiente profundizar en el tipo de instituciones de seguridad relacionadas con cada nivel: una posibilidad que se abre es la existencia de fuerzas de seguridad intermedias, que se hagan cargo de aquellas amenazas a la seguridad interior que hayan superado el nivel de la seguridad pública. Al mismo tiempo, cobra importancia la institucionalidad superior de la seguridad nacional, en línea con lo expuesto por Navarro Meza[102], o una arquitectura de seguridad nacional. Si la seguridad nacional se compone de diversos niveles relacionados entre sí, es indispensable la coordinación entre todas las agencias involucradas en estos. Por último, se debe investigar más profundamente la relación entre fenómenos como los enclaves criminales y la seguridad nacional, con tal de poder identificar los riesgos y las amenazas a tiempo.

102 NAVARRO, Miguel. 2019. "La institucional superior, el eslabón débil de la Seguridad y la Defensa en Chile". En: CUERPO ACADÉMICO. *Antecedentes para el Debate acerca de una Estrategia de Seguridad* Nacional, N° 45. ANEPE. pp. 101-164. Disponible en: file:///C:/Users/lrojas/Downloads/LIBRO-ANEPE-45-1.pdf

REFERENCIAS BIBLIOGRÁFICAS

ALCÁNTARA, Suzzete y ARVIZU, Juan. 2019. Ley de Seguridad Interior de EPN es desechada. *El Universal*. 18 de noviembre de 2019. Disponible en: https://www.eluniversal.com.mx/nacion/ley-de-seguridad-interior-de-epn-es-desechada/

ARANCIBIA, Daniel. 2020. "Relevancia Constitucional de las FF.AA.: Una Visión Actualizada". En: *Anuario de Cuadernos de Trabajo 2020*. CIEE-ANEPE. pp. 62-82. Disponible en: https://anepe.cl/wp-content/uploads/2021/05/Anuario-Cuadernos-de-Trabajo-2020.pdf

ARRATIA, Esteban. 2016. *Upp›s y la pacificación de las favelas en Río 2016 ¿Lecciones para Chile?* En: "Anuario de los Cuadernos de Trabajo 2016". CIEE-ANEPE.

BUNKER, Robert J. Bunker y SULLIVAN John P. 2011. Integrating feral cities and third phase cartels/ third generation gangs research: the rise of criminal (narco) city networks and BlackFor. *Small Wars & Insurgencies*. 22:5. pp. 764-786

CARVACHO, Pablo y RUFS. 2023. "Series sobre la criminalidad en Chile". Centro de Estudios Justicia & Sociedad. Disponible en: https://justiciaysociedad.uc.cl/seriessobre-la-criminalidad-en-chile/

CONVENCIÓN CONSTITUCIONAL. 2022. "Propuesta Constitución Política de la República de Chile". Disponible en: https://www.chileconvencion.cl/wp-content/uploads/2022/08/Texto-CPR-2022-entregado-al-Pdte-y-publicado-en-la-web-el-4-de-julio.pdf

CONSEJO CONSTITUCIONAL. 2023. "Propuesta Constitución Política de la República de Chile" Disponible en: https://www.procesoconstitucional.cl/docs/Propuesta-Nueva-Constitucion.pdf

ELKUS, Adam y SULLIVAN, John P. "State of Siege: Mexico's Criminal Insurgency", en: BUNKER, Robert y SULLIVAN, John P. 2012. *Mexico's Criminal Insurgency a Small Wars Journal – En Centro Anthology*. iUniverse, Inc.

Estados Unidos Mexicanos. 1917. Constitución Política de los Estados Unidos Mexicanos. 1917.

Estados Unidos Mexicanos. 2005. Ley de Seguridad Nacional.

Estados Unidos Mexicanos. 2009. Ley General de Sistema Nacional de Seguridad Pública.

Estados Unidos Mexicanos. 2017. Ley de Seguridad Interior.

FERRADA, Ernesto. 2020. "La Seguridad Nacional: ¿es necesaria su definición positiva en el derecho nacional?". *Escenarios Actuales*. 25 (2). pp. 29-48. Disponible en: https://www.ejercito.cl/descargas/desktop/NDE4

FUENTES, Claudia. 2005. "Seguridad Humana y Seguridad Nacional: Relación Conceptual y Práctica". Colección de Investigaciones Anepe, N°4.

FUENTES, Juan. 2012. Hacia una política de Seguridad Nacional: elementos para la discusión. En: *Revista Política y Estrategia*. ANEPE. 119.

GADFA, Grupo de Análisis de Fuerzas Armadas y Defensa. 2022. "Reconocimiento a convencionales que trabajaron el tema Fuerzas Armadas y Defensa Nacional". *El Mostrador*. Disponible en: https://www.elmostrador.cl/noticias/opinion/2022/09/19/reconocimiento-a-convencionales-que-trabajaron-el-tema-fuerzas-armadas-y-defensa-nacional/

GRIFFITHS Spielman, John. 2011. *Teoría de la Seguridad y Defensa en el Continente Americano, Análisis de los casos de EE.UU. de América, Perú y Chile*. Santiago: Ril Editores–USACH.

GRIFFITHS Spielman, John y TORO, Juan Pablo. 2020. *Desafíos para la Seguridad y la Defensa en el Continente Americano, 2020-2030*. Santiago: Athenalab. Disponible en: https://athenalab.org/wp-content/uploads/2020/12/libro_FFAA_athenalab.pdf

GRIFFITHS, John y MASALLERAS, Marcelo. 2022. *La Seguridad del Estado en Chile. Santiago*: Athenalab. Disponible en: https://athenalab.org/documento-de-trabajo-no18-la-seguridad-del-estado-de-chile/

GRILLO, Ioan. 2016. *Gangster Warlords: Drug Dollars, Killing Fields and the New Politics of Latin America.* London: Bloomsbury Press.

GUZMÁN Errázuriz, Jaime. 1985. "Seguridad nacional en la Constitución de 1980". *Revista de Derecho Público*. (37/38). pp. 45–65. Disponible en: https://revistaderechopublico.uchile.cl/index.php/RDPU/article/view/43698 https://doi.org/10.5354/rdpu.v0i37/38.43698

GUZMÁN Sánchez, Rubén. 2013. "La Seguridad Pública bajo la Seguridad Nacional: el eslabón roto de lo local y la desconexión con la Seguridad Ciudadana". En: ROSAS, María Cristina. *Repensando la Seguridad Nacional de México*. Centro de Estudios Navales (CESNAV).

KILCULLEN, David. 2013. *Out of the Mountains, the coming age of the urban guerrilla*. Nueva York: Oxford University Press.

MACIEL-PADILLA, Agustín. 2020. "El reto de la agenda de defensa de México: la ausencia de un enfoque integral de seguridad nacional". GRIFFITHS Spielman, John y TORO, Juan Pablo. *Desafíos para la Seguridad y la Defensa en el Continente Americano, 2020 - 2030*. Santiago: Athenalab. pp. 81 - 103. Disponible en: https://athenalab.org/wp-content/uploads/2020/12/libro_FFAA_athenalab.pdf

MARTÍ DE GIDÍ, Luz del Carmen. 2006. "La seguridad nacional y el acceso a la información pública en México". Xalapa: s.n. *Letras Jurídicas*. pp. 219-245. Disponible en: https://cdigital.uv.mx/bitstream/handle/1944/51453/MartideGidiLuz.pdf?sequence=1

MEJÍA Rosas, Jorge y WERDAN Torres, Leonardo. 2018. "Amenazas transnacionales y los roles de los ejércitos". *Los Ejércitos y el sistema internacional contemporáneo: Nuevas amenazas, tendencias y desafíos*. Escuela Superior de Guerra "General Rafael Reyes Prieto". pp. 47-92. Disponible en: https://docplayer.es/88575953-Los-ejercitos-y-el-sistema-internacional-contemporaneo.html

MOLINA, Carlos. 2008. La relación cívico-militar y su incidencia en las políticas de seguridad nacional: la experiencia chilena. *Revista Política y Estrategia N° 110.* ANEPE. pp. 15-16. Disponible en: https://www.politicayestrategia.cl/index.php/rpye/issue/view/9/1333

Ministerio de Defensa Nacional. 2017. Libro de la Defensa Nacional de Chile. Santiago de Chile. Ministerio de Defensa Nacional. Disponible en: https://www.acanav.cl/wp-content/uploads/2021/08/LibroDefensa.pdf

Ministerio de Defensa Nacional. 2021. Política de Defensa Nacional de Chile 2020. Santiago de Chile. Ministerio de Defensa Nacional. Disponible en: https://www.defensa.cl/wp-content/uploads/2023/06/POL%C3%8DTICA-DE-DEFENSA-NACIONAL-DE-CHILE-2020.pdf

MOLOEZNIK, Marcos Pablo. 2004. "Seguridad y uso de la fuerza en el Estado contemporáneo (una interpretación mexicana sobre los instrumentos coercitivos estatales)". *Revista del CESLA*, (6). pp. 29-36. Disponible en: https://www.revistadelcesla.com/index.php/revistadelcesla/article/view/275/271

MOLOEZNIK, Marcos Pablo y SUAREZ DE GARAY, María. 2012. "El proceso de militarización de la seguridad pública en México (2006-2010)". *Frontera Norte*. 24 (48). pp. 121-144. Disponible en: https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0187-73722012000200005

MOLOEZNIK, Marcos Pablo. 2016. "Seguridad Nacional". DÍAZ Fernández, A. M. *Conceptos Fundamentales de Inteligencia*. Valencia: Editorial Tirant Lo Blanch – Centro Nacional de Inteligencia de España. pp. 343 – 350.

MOLOEZNIK, Marcos Pablo. 2018a. Infantería de Marina en América Latina: pasado, presente y futuro, *Revista del Centro de Estudios Superiores Navales*, abril–junio, 39 (2). pp. 11-46. Disponible en: http://repositorio.uninav.edu.mx/xmlui/handle/123456789/486

MOLOEZNIK, Marcos Pablo. 2018b. "Presentación: Hacia una interpretación del proceso de militarización de la seguridad pública en América Latina". *Contextualizaciones Latinoamericanas*. 2 (19). pp. 1-22. Disponible en: http://contexlatin.cucsh.udg.mx/index.php/CL/article/view/7286/6432

MOLOEZNIK, Marcos Pablo. 2022. "Seguridad, Defensa e Instrumentos Coercitivos Mexicanos". Guerrero Agripino, Luis Felipe y MOLOEZNIK, Marcos Pablo. *Seguridad y monopolio de la fuerza en México, 2018-2021*. Ciudad de México: Universidad de Guanajuato. pp. 27- 66.

NAVARRO, Miguel. 2019. "La institucional superior, el eslabón débil de la Seguridad y la Defensa en Chile". En: CUERPO ACADÉMICO. *Antecedentes para el Debate acerca de una Estrategia de Seguridad* Nacional, N° 45. ANEPE. pp. 101-164. Disponible en: file:///C:/Users/Irojas/Downloads/LIBRO-ANEPE-45-1.pdf

NORTON, Richard. 2003. "Feral Cities". *Naval War College Review* 65, N° 4. pp. 97-106

ORDOÑEZ Martínez, Gustavo. 2021. "La Adopción del Concepto de Seguridad Nacional en México y América latina: Fundamentos, Límites y Perspectivas". Revista "Política y Estrategia". 137. pp. 121-146. Disponible en: https://www.politicayestrategia.cl/index.php/rpye/issue/view/37.

PÉREZ Ricart, Carlos. 2022. *Cien años de espías y drogas, la historia de los agentes antinarcóticos de Estados Unidos en México*. Ciudad de México. Debate.

PONTÓN Cevallos, J. 2014. "La militarización de la seguridad ciudadana: una tendencia regional". Entrevista con Marcos Pablo Moloeznik Gruer. *URVIO. Revista Latinoamericana De Estudios De Seguridad*. (12). pp. 143-146. Disponible en: https://www.redalyc.org/pdf/5526/552656545011.pdf

Presidencia de la República-México. 2014. Programa para la Seguridad Nacional 2014-2018. Disponible en: https://www.casede.org/index.php/biblioteca-casede-2-0/seguridad/seguridad-nacional/35-programa-para-la-seguridad-nacional-2014-2018.

República de Chile. 1874. Código Penal. 1874.

República de Chile. 1944. Decreto 2.226 Código de Justicia Militar.

República de Chile. 1975. Decreto 890 Fija Texto Actualizado de la Ley 12.927, sobre Seguridad del Estado.

República de Chile. 1980. Constitución Política de la República de Chile.

República de Chile. 1984. Ley 18.314 Determina Conductas Terroristas y fija su Penalidad.

República de Chile. 1990. Ley 18.961 Ley Orgánica Constitucional de Carabineros.

ROSAS, María Cristina. 2013. ¿Seguridad Nacional de Estado o de Gobierno? En: ROSAS, María Cristina. *Repensando la Seguridad Nacional de México*. Centro de Estudios Navales (CESNAV).

SARMIENTO Beltrán, Ángel Enrique. 2013. "Prólogo, La Seguridad Nacional Integral de México: Diagnósticos y Propuestas". Varios Autores. *La Seguridad Nacional Integral de México. Diagnósticos y Propuestas*. Centro de Estudios Superiores Navales (CESNAV-SEMAR) – Universidad del Ejército y Fuerza Aérea (UEFA-SEDENA), México D.F. P. vii.

SOLÍS Minor, Martha Patricia. 2018. "El proceso de militarización de la seguridad pública en México como resultado de la reconfiguración de la política de defensa estadounidense y el combate a las amenazas emergentes en América Latina". *Contextualizaciones Latinoamericanas*. 2 (19). pp- 1-18. Disponible en: http://contexlatin.cucsh.udg.mx/index.php/CL/article/view/7319/6438

SPD. 2024. Informe Nacional de Víctimas de Homicidios Consumados en Chile, Primer Semestre 2023. Fiscalía-SPD. Disponible en: https://prevenciondehomicidios.cl/wp-content/uploads/2024/01/Informe-Victimas-de-Homicidios-Consumados-alPrimer_Semestre_2023.pdf

SULLIVAN, John P. 2011. “From Drug Wars to Criminal Insurgency: Mexican Cartels, Criminal Enclaves and Criminal Insurgency in Mexico and Central America. Implications for Global Security”. *Working Paper No. 9, Fondation Maison des sciences de l’homme*. Disponible en: https://shs.hal.science/halshs-00694083/document

SULLIVAN, John P. 2023. “Crime wars: Operational perspectives on criminal armed groups in Mexico and Brazil”. Disponible en: https://international-review.icrc.org/articles/crime-wars-operational-perspectives-923#footnoteref2_j43abzd

VALDÉS, Guillermo. 2013. *Historia del Narcotráfico en México* (1a edición ed.). México D.F.: Aguilar.

VARAS, Augusto. 2020. “Seguridad Nacional: Un significante vacío”. *Política, Revista de ciencia política*, 58 (1). pp. 29-56. Disponible en: https://revistapolitica.uchile.cl/index.php/RP/article/view/61561/65343

VIZARRETEA Rosales, Emilio. 2013. “Estabilidad y Desarrollo Regional para la Seguridad Mexicana”. Varios Autores. *La Seguridad Nacional Integral de México*. México D.F: Secretaría de Marina - Armada de México Centro de Estudios Superiores Navales (CESNAV). pp. 61-76.

VOETEN, Teun. 2020. *Mexican drug violence: hybrid warfare, predatory capitalism and the logic of cruelty*. Xlibris.

YOPO, Mladen. 2019. “Estrategia de Seguridad: Una Agenda con los ciudadanos”. En: *Antecedentes para el Debate Acerca de una Estrategia de Seguridad Nacional, N° 45.* ANEPE. pp. 15-56. Disponible en: file:///C:/Users/lrojas/Downloads/LIBRO-ANEPE-45-1.pdf

TERRORISMO EN ECUADOR; UN RETO PARA LAS FUERZAS ARMADAS NACIONALES PARA LA APLICACIÓN DE TÁCTICAS PROPIAS DE UN CONFLICTO ASIMÉTRICO∞

MARLON F. LUNA QUIROZ•

RICARDO J. ACUÑA LÓPEZ••

RESUMEN

El terrorismo ha sido una amenaza global que impacta la seguridad y defensa de los Estados y el Ecuador no está exento de este contexto. Bajo esta premisa, se considera la definición misma del terrorismo y un análisis de su evolución en el contexto del Ecuador, abordándolo como una de las principales amenazas y desafíos que plantea. Profundiza las estrategias y tácticas empleadas por las Fuerzas Armadas del Ecuador (FF.AA.Ec), destacando un enfoque integral que abarca la disuasión, la prevención y su respuesta.

La cooperación interinstitucional nacional e internacional y las tácticas aplicadas en la lucha antiterrorista permitirán fortalecer la capacidad disuasiva de FF.AA.Ec mediante el desarrollo de habilidades militares modernas, las que se implementan con programas preventivos para desterrar las raíces del terrorismo, evidenciando la preparación efectiva en respuesta a los posibles ataques de estas organizaciones.

La complejidad de la amenaza se enfatiza en la necesidad de esfuerzos continuos e interinstitucionales para garantizar la defensa y seguridad del país, donde las acciones de las FF.AA.Ec reflejan un compromiso integral para enfrentar la amenaza terrorista, contribuyendo significativamente a la protección de la soberanía, el desarrollo y la integridad territorial del país.

• Teniente Coronel de Estado Mayor del Ejército Ecuatoriano. Licenciado en Ciencias Militares, (UFFAA ESPE-Ecuador), Magíster en Docencia Universitaria y Administración Educativa, (UTI-Ecuador), Magíster en Estrategia Militar Terrestre, (UFFAA ESPE), Diplomado Internacional en Competencias para Docentes y Formadores en la Universidad Tecnológica de Monterrey (México) – Cambridge. mflunaq@ejercito.mil.ec ORCID: https://orcid.org/0009-0003-7867-2560

•• Mayor de Material de Guerra. Licenciado en Ciencias Militares. (UFFAA ESPE), Msc. Docencia Universitaria (UFFAA ESPE), Diplomado en Gestión de Riesgos y Desastres. ANEPE. Chile, Diplomado en Gestión de proyectos. POL. Chile, Diplomado Logística. POL. Colombia, Diplomado en Competencias Docentes. (TEC. MONTERREY-México). rjacunal@ejercito.mil.ec ORCID: https://orcid.org/0009-0001-6125-7016

∞ Fecha de recepción: 080224 - Fecha de aceptación: 260624.

Palabras claves: *Terrorismo; antiterrorismo; contraterrorismo; Fuerzas Armadas; amenazas; seguridad; defensa; neutralización.*

TERRORISM IN ECUADOR; A CHALLENGE FOR THE ARMED FORCES FOR THE APPLICATION OF TACTICS IN AN ASYMMETRIC WAR

ABSTRACTS

The Terrorism has been a global threat that impacts the security and defense of States and Ecuador is not exempt from this context. Considers the very definition of terrorism and an analysis of its evolution in the context of Ecuador, addressing it as one of the main threats and challenges it poses. It deepens the strategies and tactics used by the Armed Forces, highlighting a comprehensive approach that encompasses deterrence, prevention and response.

National and international inter-institutional cooperation and the tactics applied in the fight against terrorism will allow strengthening the FF.AA.Ec deterrent capacity through the development of modern military skills, which are implemented with preventive programs to banish the roots of terrorism, evidencing effective preparation in response to possible attacks by these organizations.

The complexity of the threat is emphasized in the need for continuous and inter-institutional efforts to guarantee the defense and security of the country, where the actions of the Armed Forces reflect a comprehensive commitment to confront the terrorist threat, contributing significantly to the protection of the sovereignty, development and territorial integrity of the country.

Keywords: *Terrorism; anti-terrorism; counterterrorism; Armed Forces; threats; security; defense; neutralization.*

TERRORISMO NO EQUADOR; UM DESAFIO PARA AS FORÇAS ARMADAS NA APLICAÇÃO DE TÁTICAS EM UMA GUERRA ASSIMÉTRICA

RESUMO

O terrorismo tem sido uma ameaça global que impacta a segurança e a defesa dos Estados e o Equador não esta isento deste contexto. Sob esta premissa, considera-se a própria definição de terrorismo e uma análise de sua evolução no contexto do Equador, abordando-o como uma das principais ameaças e desafios que representa. Aprofunda

as estratégias e táticas utilizadas pelas Forças Armadas do Equador (FF.AA.Ec), destacando uma abordagem abrangente que abrange dissuasão, prevenção e resposta.

A cooperação interinstitucional nacional e internacional e as tácticas aplicadas no combate ao terrorismo reforçarão a capacidade dissuasora das Forças Armadas através do desenvolvimento de competências militares modernas, que são implementadas com programas preventivos para banir as raízes do terrorismo, evidenciando uma preparação eficaz na resposta a possíveis ataques destas organizações.

A complexidade da ameaça é enfatizada na necessidade de esforços contínuos e interinstitucionais para garantir a defesa e segurança do país, onde a atuação das Forças Armadas reflete um compromisso abrangente de enfrentamento à ameaça terrorista, contribuindo para a proteção de a soberania, o desenvolvimento e a integridade territorial do país.

Palavras-chave: *Terrorismo; antiterrorism; contraterrorismo; Forças Armadas; ameaças; segurança; defesa; neutralização.*

I. INTRODUCCIÓN

La persistente crisis de seguridad en el Ecuador, marcada por enfrentamientos entre organizaciones criminales vinculadas al narcotráfico, plantea desafíos inminentes que requieren una evaluación crítica. La escalada de violencia, evidenciada por eventos como las masacres carcelarias y el aumento de homicidios, destaca la necesidad de comprender el papel crucial que desempeñan las Fuerzas Armadas con todas sus acciones para minimizar las amenazas terroristas y garantizar la seguridad integral nacional.

Desde la década de 1990 hasta hoy, el Ecuador ha experimentado actos terroristas liderados por grupos de izquierda, evolucionándose hacia la amenaza actual dentro de los Grupos Delincuenciales Organizados (GDO). Las Fuerzas Armadas ecuatorianas (FF.AA.Ec), en colaboración con la Policía Nacional están en la vanguardia de la defensa, encargadas de salvaguardar la seguridad interna, la soberanía y la integridad territorial, así como de proteger a la población civil ante posibles actos terroristas como parte de la seguridad integral. Este contexto subraya la necesidad de examinar la eficacia de las estrategias implementadas por las FF.AA.Ec y su impacto en la seguridad y defensa nacional.

El objetivo de esta investigación es proporcionar una comprensión integral de cómo las tácticas y estrategias que se implementen en las FF.AA.Ec, en un conflicto asimétrico, contribuyen a la lucha contra el terrorismo realizando una postulación de la efectividad de las estrategias implementadas por las FF.AA.Ec, e identificar los desafíos enfrentados, permitiendo realizar las recomendaciones para fortalecer una capacidad de respuesta integral ante una amenaza terrorista. La interrogante: *¿Cómo pueden las acciones de las Fuerzas Armadas Ecuatorianas adaptarse y contrarrestar eficazmente esta evolución de la amenaza terrorista?,* tiende a enfatizar la importancia de la planificación, ejecución y adaptabilidad,

en el contexto de la seguridad integral que convergen en la coordinación interinstitucional, la inteligencia militar, el respeto a los derechos humanos y la actuación gubernamental responsable, elementos cruciales en la respuesta política, estratégica y táctica en la lucha contra el terrorismo en el Ecuador.

La importancia del estudio arranca con las bases conceptuales de la amenaza, donde se induce desde la perspectiva de seguridad y defensa, relacionándola con las tácticas y estrategias militares entrelazadas con la adecuada planificación, ejecución y adaptabilidad de las acciones en coordinación con otras instituciones estales, bajo los conceptos claves de adaptabilidad de las estrategias militares, coordinación interinstitucional, gobernanza, respeto a los derechos humanos, entre otros.

Para el desarrollo del artículo se emplea una investigación de carácter descriptiva, basada en la revisión bibliográfica documental de fuentes primarias, que constituyen la base del análisis integral y contextualizado del accionar de Fuerzas Armadas en función de la seguridad interna, considerando hechos que constituyen hitos en la planificación de las acciones para el desarrollo de las estrategias antiterroristas, que serán presentadas en las conclusiones.

II. MATERIALES Y MÉTODOS

Para abordar esta investigación sobre las acciones de las Fuerzas Armadas del Ecuador en la lucha contra el terrorismo, desde la perspectiva de la seguridad y la defensa, se empleó un enfoque mixto que combinó métodos cualitativos y cuantitativos. Esto permitió una comprensión integral de las estrategias militares y su impacto en la seguridad nacional.

Se aplicó un método deductivo, partiendo de la teoría existente sobre seguridad y defensa para analizar la efectividad de las acciones antiterroristas de las Fuerzas Armadas ecuatorianas. Además, se utilizó un método comparativo para evaluar diferentes períodos y enfoques estratégicos a lo largo del tiempo.

2.1. Técnicas e Instrumentos

2.1.1. Revisión documental: Se realizó un análisis exhaustivo de documentos oficiales, informes de inteligencia, y doctrinas militares enfocadas en las acciones antiterroristas en Ecuador. Este análisis permitió comprender las políticas, estrategias y operativos específicos implementados para contrarrestar las amenazas terroristas, basándose en fuentes documentales verificables y accesibles públicamente.

2.1.2. Análisis estadístico de datos públicos: Se recopiló y analizó información cuantitativa disponible públicamente sobre incidentes terroristas y operaciones de respuesta. La aplicación de técnicas estadísticas avanzadas permitió identificar tendencias, patrones y correlaciones significativas que arrojan luz sobre la efectividad de las estrategias antiterroristas. La base de datos incluyó informes gubernamentales, estudios académicos previos y estadísticas oficiales.

2.1.3. Consulta de expertos a través de fuentes secundarias: Para complementar el análisis documental y estadístico, se revisaron estudios, análisis y opiniones de expertos en seguridad y defensa publicados en literatura académica y en medios especializados. Aunque no se realizaron entrevistas directas, la información recabada de estas fuen-

tes secundarias proporcionó valiosas perspectivas cualitativas sobre las tácticas y desafíos enfrentados.

2.1.4. Población: La población objetivo incluyó miembros activos de las Fuerzas Armadas ecuatorianas, expertos en seguridad y defensa, y documentos gubernamentales relevantes. Con representantes de diferentes periodos históricos, unidades militares y perspectivas profesionales.

2.2. Procedimientos

2.2.1. Selección y categorización de documentos: Se implementó un riguroso proceso para la selección y categorización de los documentos relevantes, utilizando criterios claros de inclusión basados en la relevancia, fecha de publicación y la autoridad de la fuente. Este enfoque sistemático aseguró que solo se incorporara información fiable y pertinente al estudio.

2.2.2. Análisis documental: Cada documento seleccionado fue sometido a un detallado análisis cualitativo para extraer información clave relacionada con las estrategias antiterroristas implementadas, los resultados obtenidos y los desafíos enfrentados. Este análisis involucró la identificación de temas comunes, discrepancias y la evaluación de la evolución de las tácticas a lo largo del tiempo.

2.2.3. Evaluación: Se emplearon metodologías estadísticas apropiadas para el análisis de los datos cuantitativos recopilados, incluyendo análisis de varianza, correlación y regresión, entre otros. Esto permitió una evaluación objetiva de la efectividad de las respuestas antiterroristas y la identificación de factores clave que influyen en los resultados.

Este enfoque metodológico proporciona un marco integral para evaluar la efectividad de las acciones de las Fuerzas Armadas ecuatorianas contra el terrorismo, garantizando la validez y confiabilidad de los resultados obtenidos.

III. RESULTADOS Y ANÁLISIS

3.1. Marco teórico y contexto geopolítico

El Ecuador ha sido históricamente un país caracterizado por su estabilidad política y una baja incidencia de terrorismo. Sin embargo, en los últimos años, ha habido preocupaciones crecientes sobre la infiltración de grupos delincuenciales organizados y la posibilidad de actividades relacionadas con el terrorismo debido a su ubicación geográfica estratégica en América Latina. Estos grupos, incluyendo carteles de la droga y pandillas locales, han representado un desafío para la seguridad interna del país y han requerido una respuesta gubernamental efectiva.

El Ecuador, situado en la costa noroeste de América del Sur, comparte fronteras con Colombia y Perú, dos países que han experimentado conflictos relacionados con el narcotráfico y el terrorismo en el pasado. La ubicación geográfica de Ecuador como puente entre los países productores de drogas en América del Sur y los mercados de consumo en el norte ha llevado a preocupaciones de seguridad y ha requerido una estrecha cooperación con agencias internacionales de aplicación de la ley. Además, la estabilidad política y económica

de Ecuador se ha convertido en un factor crucial en el panorama geopolítico de América Latina, influyendo en sus relaciones con otras naciones de la región y actores internacionales. La respuesta del gobierno ecuatoriano a los desafíos de seguridad, incluyendo la lucha contra los grupos delincuenciales organizados, es esencial para mantener su estabilidad interna y su posición en la comunidad internacional.

Según datos del Banco Mundial, Ecuador ha enfrentado desafíos económicos significativos en los últimos años, incluyendo la dependencia del petróleo, la falta de amortiguadores macroeconómicos y una serie de barreras estructurales que han obstaculizado el crecimiento económico y la reducción de la pobreza en el país[1]. La economía de Ecuador se ha desacelerado debido a factores como el crimen organizado, disrupciones en la producción de petróleo, eventos climáticos e incertidumbre política[2]. El nuevo gobierno enfrenta restricciones de liquidez, déficit fiscal y la necesidad de implementar reformas estructurales[3]. En este contexto, el análisis de la efectividad de las estrategias de las Fuerzas Armadas del Ecuador, como se aborda en el presente artículo, cobra relevancia al considerar cómo estas estrategias pueden contribuir a abordar no solo las amenazas terroristas, sino también los desafíos económicos y sociales que enfrenta Ecuador.

3.2. Teorías clave en Seguridad y Defensa

En el ámbito de la seguridad y defensa, teorías como el Realismo, el Constructivismo y el Humanismo ofrecen distintas perspectivas. El Realismo, enfocado en el poder estatal y la seguridad nacional, es particularmente relevante para Ecuador, dada su historia de conflictos fronterizos y la necesidad de proteger su soberanía. El Constructivismo, que subraya la importancia de las normas y la identidad, se refleja en cómo Ecuador aborda los desafíos de seguridad en un contexto regional. El Humanismo, que pone énfasis en los derechos humanos y la seguridad humana, es esencial para entender la respuesta de Ecuador a las amenazas asimétricas internas y transnacionales.

3.2.1. Conceptualización asociada al terrorismo

Antes de iniciar con una conceptualización del terrorismo es necesario plasmar algunas definiciones fundamentales, que permitan esclarecer de mejor forma el desarrollo del presente artículo, de esta manera se permitirá tener una mejor aserción y entendimiento del abordamiento del tema en conceptos como amenaza, terrorismo, antiterrorismo, contraterrorismo y neutralización.

- *Amenaza*: Capacidad potencial de un actor de causar daño sobre objetivos específicos, representa un peligro latente que puede materializarse en acciones violentas. Refleja la importancia de identificar y entender el potencial daño que representan los grupos terroristas para acciones violentas.

1 BANCO MUNDIAL. Ecuador: panorama general [en línea]. [Fecha de consulta: 2 abril 2024]. Disponible en: https://www.bancomundial.org/es/country/ecuador/overview

2 GRIES, Thomas y REDLIN, Maiken. Las raíces del terrorismo: una investigación cuantitativa sobre las causas socioeconómicas de la actividad terrorista. Revista de Política y Gobierno. 2019. Vol. 26, no. 1, pp. 59-81. ISSN 1665-2037.

3 MARTÍNEZ Muñoz, Pablo. Las fuerzas armadas de Ecuador y su rol en la lucha contra el crimen organizado transnacional. Revista Científica General José María Córdova. 2017. Vol. 15, no. 20, pp. 67-88. ISSN 1900-6586.

- *Terrorismo***:** Forma de violencia política ejercida por actores no estatales contra la población civil con la intención de infundir temor para alcanzar objetivos ideológicos, políticos o sociales, aprovechando la vulnerabilidad de las sociedades abiertas.

- *Antiterrorismo* y *contraterrorismo***:** Conjunto de técnicas, tácticas, procedimientos y estrategias de medidas ofensivas de los Estados para prevenir, disuadir y responder a los actos terroristas, incluye acciones encubiertas, operativos especiales, inteligencia y uso de la fuerza. Representan las estrategias y tácticas a ser implementadas para prevenir (antiterrorismo) y responder activamente (contraterrorismo) a los actos terroristas.

- *Neutralización*: Conjunto de acciones encaminadas a eliminar o reducir significativamente la capacidad operativa de grupos armados irregulares y organizaciones terroristas. Se relaciona con las acciones específicas de las FF.AA.Ec para disminuir o eliminar la capacidad operativa de los terroristas, siendo un indicador clave de la efectividad de sus estrategias.

Cada uno de estos conceptos aporta a la comprensión integral de cómo las FF. AA. del Ecuador implementarán las estrategias para neutralizar las acciones de grupos enmarcadas en acciones de terrorismo, permitiendo evaluar la efectividad en el campo de la seguridad y defensa.

3.3. El terrorismo y la evolución de sus actos y acciones en el Ecuador

Esta amenaza asimétrica conocida como prácticas terroristas, están estratégicamente dirigidas al menoscabo y a la destrucción de la estructura de poder de un determinado sistema social, usando la violencia como herramienta política, desafiando sus valores y principios[4]. Las actividades que los identifica se ligan a la amenaza de la integridad territorial y la seguridad de los Estados, se orientan a destruir el Estado de derecho, así como las libertades fundamentales y atentar, por lo tanto, contra la democracia.

El Protocolo adicional a los Convenios de Ginebra de 1949 relativo a la protección de las víctimas de los conflictos armados internacionales manifiesta: "Quedan prohibidos los actos o amenazas de violencia cuya finalidad principal sea aterrorizar a la población civil"[5]. Esto nos lleva a reflexionar sobre la cuestión de la legitimidad del terrorismo como método político. Las prácticas terroristas constituyen la antítesis de la violencia legítima, que lejos de justificarse en sí misma, responde ante ciertos límites éticos y jurídicos (marcos normativos, sistemas penales, etc.)[6]. En la política como vocación, Max Weber formuló la definición clásica del Estado como entidad con el monopolio del uso legítimo de la violencia dentro de los límites de un territorio determinado: (El Estado se ha visto como un único otorgante del "derecho" de la fuerza física), es decir, solo quien tiene el poder de ejercerla o de permitir

4 SCHMID, Alex P. y JONGMAN, Albert J. Political terrorism: a new guide to actors, authors, concepts, data bases, theories, and literature. Amsterdam: North-Holland, 1988. 695p. ISBN 0-444-85659-3

5 COMITÉ INTERNACIONAL DE LA CRUZ ROJA. Protocolo adicional a los Convenios de Ginebra de 1949 relativo a la protección de las víctimas de los conflictos armados internacionales (Protocolo I). Ginebra: CICR, 1977. Título IV, sección I, capítulo II, art. 51.

6 WEBER, Max. La política como vocación. Madrid: Alianza Editorial, 2009. 188p. ISBN 978-84-206-6061-0.

a grupos o individuos que la ejerzan en su nombre[7]. Una parte fundamental del poder del Estado proviene de su capacidad para establecer su legitimidad.

La globalización, los cambios acelerados y la evolución tecnológica han permitido que este tipo de amenaza haya progresado su accionar, al igual que lo han hecho la mayoría de las actividades humanas, sobrepasando la era digital denominado Ciberterrorismo, la cual representa una vulnerabilidad a la seguridad y defensa del Estado y "(…) Ecuador no se excluye de esto por el fácil acceso que tienen actores estatales y no estatales a estas tecnologías, quienes han innovado sus técnicas tácticas y procedimientos, ocasionado incidentes cibernéticos en la infraestructura crítica del Estado, afectación en operaciones militares y delitos cibernéticos"[8].

Los grupos terroristas utilizan muchas formas de violencia ilegal o amenaza de uso de la violencia para infundir miedo y coaccionar a los gobiernos y las sociedades promoviendo una variedad de ideologías políticas, sociales, criminales, económicas y religiosas[9]. Los grupos terroristas pueden amenazar los intereses y la seguridad del Estado y se caracterizan por ser una amenaza (intención, capacidad y motivación) que comprende:

- Objetivo: Político, sin lucro.
- Método: Uso de la violencia y el terror.
- Medios: No combatientes o víctimas civiles.
- Actor(es): Individuos no estatales o grupos organizados.

A nivel mundial, el terrorismo ha sido una preocupación constante para muchos países. Organizaciones como Al Qaeda, ISIS (Estado Islámico) y Boko Haram han llevado a cabo ataques mortales en diferentes partes del mundo, principalmente en Oriente Medio, Europa y África[10]. Estas organizaciones tienen motivaciones políticas y religiosas, y buscan imponer su ideología a través de la violencia[11].

En Ecuador, la presencia y evolución de Grupos Delincuenciales Organizados (GDO) ha marcado significativamente la seguridad y estabilidad del Estado en las últimas décadas. Estos grupos, integrados en el tejido del narcotráfico y actividades del crimen organizado transnacional, han escalado los niveles de violencia y criminalidad, generando un entor-

7 WEBER, Max. Economía y sociedad: esbozo de sociología comprensiva. México D.F.: Fondo de Cultura Económica, 2014. 1245p. ISBN 978-84-375-0728-7

8 ESTADO MAYOR CONJUNTO DE LAS FUERZAS ARMADAS DEL ECUADOR. Plan Estratégico Institucional de FF.AA. 2021-2033. Quito, 2021. p. 52.

9 HOFFMAN, Bruce. Inside terrorism. New York: Columbia University Press, 2006. 456 p. ISBN 978-0-231-12699-9.

10 CRONIN, Audrey Kurth. How al-Qaeda ends: the decline and demise of terrorist groups. International Security. 2006, vol. 31, no. 1, pp. 7-48. ISSN 0162-2889.

11 STERN, Jessica. Terror in the name of God: why religious militants kill. New York: Ecco, 2003. 352 p. ISBN 978-0-06-050528-8.

no de preocupación tanto a nivel nacional como internacional[12]. Este fenómeno ha evolucionado desde acciones aisladas hasta constituir una amenaza concreta para la seguridad nacional, desafiando la capacidad del Estado y las Fuerzas Armadas para su contención y neutralización.

La respuesta del Estado ecuatoriano ante este escenario ha necesitado adaptarse a la cambiante naturaleza del terrorismo, empleando estrategias de conflicto asimétrico que van desde la inteligencia militar hasta operaciones de contrainsurgencia. Estas acciones han sido cruciales para desmantelar la infraestructura terrorista y mitigar su impacto en la población civil. Sin embargo, esta adaptación ha enfrentado retos significativos en términos de recursos, entrenamiento y doctrina militar, resaltando la importancia de una cooperación internacional fortalecida y un enfoque multidimensional.

El surgimiento de células terroristas radicales dentro de la sociedad ecuatoriana, como el «Movimiento Guevarista Tierra y Libertad», ha expuesto la complejidad de la amenaza terrorista. Este fenómeno no solo opera en las sombras, sino que también busca infiltrarse en el tejido social y político del país. Tal situación ha requerido del Estado una respuesta más sofisticada que trasciende la confrontación armada, incorporando estrategias para contrarrestar la radicalización y el reclutamiento de jóvenes ecuatorianos[13].

Esta compleja dinámica regional, donde el Estado ecuatoriano y sus Fuerzas Armadas enfrentan el desafío de adaptarse a un entorno de seguridad en constante cambio, subraya la necesidad de un enfoque integral. Dicho enfoque debe combinar capacidades militares con iniciativas de desarrollo social, fortalecimiento institucional y cooperación internacional, para asegurar la paz y la seguridad tanto a nivel nacional como regional. En este contexto, el terrorismo en Ecuador refleja un escenario donde las estrategias y tácticas deben evolucionar para enfrentar eficazmente esta amenaza multifacética.

Este escenario ha propiciado una estrecha colaboración entre las Fuerzas Armadas y la Policía Nacional, uniendo sus esfuerzos para llevar a cabo operaciones destinadas a combatir actos clasificados como terrorismo. Es crucial destacar que la seguridad se ha convertido en un eje fundamental en los últimos años, especialmente donde el Ecuador ha sido víctima de una serie de incidentes y acciones con connotaciones terroristas, que han erosionado la estabilidad y la seguridad del Estado. La siguiente tabla presenta una cronología de eventos y actos con peculiaridades terroristas que han permitido visualizar la urgente necesidad de una estrategia integral de seguridad y defensa que involucre a las Fuerzas Armadas del Ecuador en una colaboración coordinada y planificada con otras instituciones del Estado.

12 CARRASCO, J. y PILALUMBO, W. (2022). *Guerra de cuarta generación en la frontera norte ecuatoriana*. Revista de la Academia de Guerra del Ejército Ecuatoriano, vol. 15, no. 1, pp. 13-13. ISSN 26005697. DOI 10.24133/AGE.N15.2022.07.

13 Ibíd.

Tabla 1
Cronología de eventos de actos y acciones tipo terrorista en el Ecuador

FECHA	EVENTO
27 de enero de 2018	Miembros del Grupo Irregular Armado del Frente "Oliver Sinisterra" (FOS) llevaron a cabo un atentado terrorista al detonar un coche bomba cerca del distrito de la Policía Nacional de San Lorenzo, en Esmeraldas. Este acto provocó heridas en 23 personas y causó daños tanto en la infraestructura policial como en 37 viviendas circundantes.
16 de marzo de 2018	Se produjo un atentado contra el Retén Naval de Borbón, ubicado en el cantón Eloy Alfaro, Esmeraldas, con reporte de daños materiales.
18 de marzo de 2018	Se reportó una explosión en el recinto de Durango, Parroquia Santa Rita, dirigida contra un vehículo de la Policía Nacional en el cantón San Lorenzo, Esmeraldas, resultando en daños materiales.
26 de marzo de 2018	• Miembros del Grupo Irregular Armado "Oliver Sinisterra" secuestraron y posteriormente asesinaron a los periodistas del equipo de El Comercio, quienes se encontraban realizando una cobertura sobre los eventos en curso en Mataje y sus alrededores. • Individuos vinculados al Grupo Irregular Armado "Oliver Sinisterra" hicieron estallar un artefacto explosivo en el lado de la carretera San Lorenzo-Mataje, resultando en la trágica pérdida de tres infantes de marina y dejando a siete personas heridas.
07 y 29 de mayo de 2019	Se produjo la detonación de varios artefactos explosivos en las instalaciones de la Universidad Estatal de Guayaquil, generando únicamente daños materiales. Hasta el momento no se ha logrado identificar a los posibles responsables de este incidente.
Del 02 al y 13 de octubre de 2019	En octubre de 2019, Ecuador fue testigo de intensas protestas que buscaban el derrocamiento del Gobierno constituido legalmente. Estas manifestaciones, inicialmente de resistencia, evolucionaron hacia actos vandálicos y terroristas, marcados por ataques e incendios a vehículos militares, toma de gobernaciones, daños a antenas de transmisión, asaltos y saqueos a empresas. La situación alcanzó su punto crítico con el incendio de las instalaciones de la Contraloría General y un ataque a Teleamazonas. Estos eventos revelaron no solo una profunda división en la sociedad ecuatoriana, sino también la comisión de delitos de rebelión y terrorismo por parte de grupos como el Pmcle, Vientos de Pueblo, Juventud Guevarista, Comités de la Revolución Ciudadana y Guardia Indígena.

23 de febrero de 2021	Se desencadenó una masacre carcelaria en Ecuador, dejando un saldo de 79 reclusos asesinados simultáneamente en los Centros de Rehabilitación Social de Turi, del Litoral, de Latacunga y de Guayas. Las cifras resultan impactantes, superando el número total de fallecidos en todas las prisiones del país el año anterior. Los enfrentamientos entre bandas rivales amotinadas en Cuenca, Guayaquil y Latacunga revelaron una violencia extrema, evidenciada por imágenes de cuerpos decapitados y desmembrados que circularon en redes sociales.
21 de julio de 2021	Masacres simultáneas en las cárceles de Guayaquil y Latacunga dejaron 27 reos muertos. Los conflictos iniciaron por ataques entre Los Choneros y Los Lobos en la Penitenciaría del Litoral.
21 de enero de 2022	En el sur de Guayaquil, en el sector de la "Playita del Guasmo", se llevó a cabo un atentado en el que 15 individuos llegaron en lanchas rápidas y dispararon contra personas en una cancha deportiva. Este incidente resultó en 5 fallecidos y 9 personas heridas.
14 de febrero de 2022	Dos cuerpos fueron encontrados colgados de un puente peatonal en Durán. Ambas víctimas tenían antecedentes penales relacionados con narcotráfico.
20 de febrero de 2022	Un hombre de 21 años fue abandonado en el norte de Guayaquil con un explosivo en la cabeza que detonó, dispersando sus restos en un radio de 30 metros.
25 de abril de 2022	Se produjo un atentado con coche bomba en las cercanías del Centro de Rehabilitación Social del Litoral y el Centro de Máxima Seguridad La Roca. Además, hubo enfrentamientos entre las bandas Los Choneros y Latin Kings en el Centro de Rehabilitación Social El Inca en Quito, resultando en la muerte de 15 reclusos.
04 de febrero de 2023	La noche antes de las elecciones del 5 de febrero de 2023, Omar Menéndez, candidato a la Alcaldía de Puerto López por el Movimiento Revolución Ciudadana, fue asesinado mientras organizaba los preparativos con su comitiva.
20 de marzo de 2023	Lenin Artieda, periodista de Ecuavisa, recibió una memoria USB con un dispositivo oculto que explotó al insertarlo en una computadora. Otros periodistas de varios medios también recibieron sobres similares.
24 de julio de 2023	En Tonchigüe, Esmeraldas, una balacera dejó dos muertos y cuatro heridos. Se arrojaron panfletos amenazantes en dos medios de comunicación con consignas contra la paz social.

09 de agosto de 2023	Fernando Villavicencio, candidato presidencial en las elecciones anticipadas de 2023, fue asesinado después de un mitin al norte de Quito. En el ataque resultaron heridos una candidata a asambleísta y dos policías, y uno de los sicarios murió más tarde.
08 de septiembre de 2023	El concejal electo Bolívar Vera de Durán para el período 2023-2027 fue asesinado, tras ser secuestrado y torturado por criminales asociados al narcotráfico.
01 de octubre de 2023	Individuos desconocidos arrojaron un artefacto explosivo en el patio de una escuela privada en la cooperativa Unión de Bananeros, al sur de Guayaquil, al detonar el dispositivo no causó daños materiales ni de personas.
07 de octubre de 2023	Seis ciudadanos colombianos implicados en el asesinato de Fernando Villavicencio fueron encontrados muertos en la Penitenciaría del Litoral en Guayaquil, donde cumplían prisión preventiva por el crimen del ex-candidato presidencial.
07 de enero 2024	Las autoridades ecuatorianas confirmaron la evasión de Adolfo Macías, alias "Fito", líder presumido de Los Choneros, de la prisión de Guayaquil. Este grupo, notorio y temido, está implicado en el narcotráfico transnacional, operando en colaboración con el cártel de Sinaloa y el Frente Oliver Sinisterra, según Insight Crime.
09 de enero 2024	Durante una emisión en directo, individuos encapuchados y armados irrumpieron en el canal TC Televisión de Guayaquil, tomando como rehenes a empleados y sembrando el pánico con disparos, según revelan imágenes y videos circulados en redes. La Policía de Ecuador respondió rápidamente, ejecutando un amplio operativo que culminó con la detención de varios sospechosos y la recolección de evidencia relacionada con el incidente.

Fuente: Autores

3.3.1 Resultados de las acciones de las Fuerzas Armadas del Ecuador en la lucha contra el terrorismo

Entre 2022 y 2024, las Fuerzas Armadas del Ecuador (FF.AA.Ec) redoblaron sus esfuerzos contra el terrorismo, centrándose en desmantelar redes vinculadas al narcotráfico y crimen organizado transnacional. Estas operaciones, esenciales para la seguridad nacional, han fortalecido la soberanía e integridad territorial del país. Un hito en estas operaciones fue el decomiso en Vinces, Los Ríos, de 22 toneladas de droga, demostrando la efectividad de las FF.AA.Ec en la lucha contra amenazas complejas[14].

14 MINISTERIO DE DEFENSA NACIONAL. (2023). *Informe de Gestión CCFFAA*. Quito: Ministerio de Defensa Nacional.

El compromiso del Estado en enfrentar estas amenazas se manifiesta en los decretos ejecutivos emitidos por el presidente Daniel Noboa Azín. En el Decreto Ejecutivo No. 111, Noboa Azín delineó una estrategia integral basada en el derecho internacional humanitario y la movilización de las FF. AA. y la Policía Nacional para contrarrestar actos de violencia que desafían la democracia y el Estado de derecho, reflejando la determinación de Ecuador por proteger a sus ciudadanos y mantener la estabilidad democrática[15].

Los resultados de las operaciones militares y la cooperación interinstitucional durante este periodo incluyen:

- Destrucción de más de 1.896 armas, 6.798 accesorios de armas y 2.928 municiones.
- Decomiso de armas de corto y largo alcance en contenedores contaminados.
- Operaciones militares coordinadas con la Policía Nacional para combatir el terrorismo y la delincuencia.
- Captura de integrantes de diferentes grupos delictivos organizados vinculados al narcotráfico.
- Decomiso de más de 30.000 municiones, armas y granadas.

Estas acciones evidencian el firme compromiso y la determinación de las Fuerzas Armadas ecuatorianas en su lucha contra el terrorismo, priorizando la protección de la soberanía y la integridad del país[16].

La consolidación de las políticas de seguridad bajo la administración del Presidente de la República del Ecuador, Daniel Noboa Azín, particularmente a través de los Decretos Ejecutivos No. 110 y No. 111, ha permitido una respuesta estatal robusta y articulada frente a las amenazas de terrorismo. Estas políticas no solo reflejan un enfoque proactivo hacia la seguridad y la defensa nacional sino también el compromiso de Ecuador con el mantenimiento de la paz y el orden público, asegurando así el bienestar y la protección de sus ciudadanos frente a desafíos de magnitud sin precedentes. La actuación de las Fuerzas Armadas, en estrecha colaboración con la Policía Nacional, subraya la capacidad de Ecuador para enfrentar y neutralizar amenazas latentes, reafirmando su posición en la lucha global contra el terrorismo y el crimen organizado.

15 NOBOA AZÍN, Daniel. (2024). *Decreto Ejecutivo No. 111*. Quito: Presidencia de la República del Ecuador.

16 COMANDO CONJUNTO DE LAS FUERZAS ARMADAS. (2022). *Plan Estratégico Institucional 2021-2025*. Quito: Comando Conjunto de las Fuerzas Armadas del Ecuador.

Tabla 2
Operaciones y resultados durante la vigencia del Decreto Ejecutivo 411[17]

OPERACIONES EJECUTADAS	CANTIDAD
Operaciones	249.814
RESULTADOS	
Vehículos registrados	2’144.478
Personas registradas	2’148.810
Motos retenidas	1.080
Registro de personas (Migración)	57
Nichos criminales intervenidos	17
Personas detenidas	5.571
Vehículos retenidos	673
Armas de fuego (unidades)	719
Citaciones entregadas por tránsito	487
Desarticulación de GDO (Grupos Delictivos Organizados)	59
Motos recuperadas	358
Carros recuperados	315
Controles vehiculares realizados por tránsito	529
Sustancias sujetas a fiscalización SSF (kilogramos)	15.981,33

Fuente: Informe de Gestión del Comaco 2022: Resultados en las operaciones - Dirección de Operaciones del CC.FF.AA.

17 REPÚBLICA DEL ECUADOR. (2022a). *Decreto Ejecutivo 411, 30 de abril de 2022*. Se declara el estado de excepción por grave conmoción interna por razones de seguridad ciudadana en las provincias de Guayas, Esmeraldas y Manabí. Quito: Registro Oficial.

Tabla 3
Operaciones y resultados durante la vigencia de los Decretos Ejecutivos 527 y 561[18]

OPERACIONES EJECUTADAS	CANTIDAD
Operaciones de ámbito interno (apoyo PPNN, operaciones (CAMEX)	8.457
RESULTADOS	
Personas registradas	440.421
Desarticulación de GDO	64
Munición decomisada	11.681
Sustancias sujetas a fiscalización (gr)	15.945.083,7
Armas de fuego incautadas (largas)	36
Armas de fuego incautadas (cortas)	386
Armas de fuego entregadas a Control de Armas	8
Detenidos por delitos	1.498
Vehículos recuperados	144
Explosivo decomisado	136
Control de centros de diversión	254
Retiro de libadores	30.798
Detenidos por boletas de captura	73
Armas blancas decomisadas	2.049
Motos recuperadas	116
Motos retenidas por orden municipal	5.909

Fuente: Informe de Gestión del Comaco 2022: Resultados en las operaciones - Dirección de Operaciones del CC.FF.AA.

18 REPÚBLICA DEL ECUADOR. (2022b). *Decreto Ejecutivo 527 y 561, 14 de agosto de 2022*. Se declara el estado de excepción en el Distrito Metropolitano de Guayaquil, Durán, Samborondón y Guayaquil, por incremento de actividades delictivas. Quito: Registro Oficial.

Tabla 4
Operaciones y resultados durante la vigencia de los Decretos Ejecutivos 588 y 589[19]

OPERACIONES EJECUTADAS	CANTIDAD
Operaciones CAMEX	8.187
RESULTADOS	
Armas de fuego incautadas (unidades)	128
Armas blancas decomisadas (unidades)	409
Explosivos tacos de dinamita	9
Munición (unidades)	2.053
Personas registradas	115.777
Vehículos registrados	67.330
Sustancias sujetas a fiscalización (gr)	11.721
Personas aprehendidas	146

Fuente: Informe de Gestión del Comaco 2022: Resultados en las operaciones - Dirección de Operaciones del CC.FF.AA.

Estos resultados revisados muestran que las operaciones militares en el Ecuador han tenido consecuencias tangibles en la reducción de actos terroristas y en el fortalecimiento de la seguridad nacional. Estas acciones han sido cruciales en la desarticulación de células terroristas, cabe mencionar que estas decantan en las lecciones aprendidas para llevar la ejecución de operaciones con un enfoque más holístico, buscando equilibrar la seguridad, el respeto a los derechos humanos y la estabilidad política, sugiriendo áreas de mejora en la coordinación interinstitucional y la participación comunitaria.

La pregunta fundamental que surge al momento es: ¿Cómo pueden las acciones de las Fuerzas Armadas ecuatorianas mudarse y adaptarse para contrarrestar eficazmente la evolución de una amenaza terrorista?, pues bien, esta hipótesis enfatiza la importancia de la planificación, ejecución y adaptabilidad, de tácticas, técnicas y estrategias como parte de la seguridad integral, que se requieren de acciones urgentes para mantener la seguridad y defensa del Ecuador en la lucha contra el terrorismo.

19 REPÚBLICA DEL ECUADOR. (2022c). *Decreto Ejecutivo 588 y 589, 01 y 04 de noviembre de 2022*. Se declara el estado de excepción en las provincias de Guayas, Esmeraldas y Santo Domingo por homicidios, asesinatos y sicariatos. Quito: Registro Oficial.

3.4. Desafíos del terrorismo en la legislación del Ecuador

El Código Orgánico Integral Penal (COIP) de Ecuador, específicamente en su artículo 366, define el terrorismo como la acción cometida por individuos o asociaciones armadas que buscan provocar o mantener en estado de terror a la población o a un sector de ella. Sin embargo, esta definición ha sido objeto de crítica por su indeterminación y la discrecionalidad que permite en su aplicación, lo que representa un desafío fundamental dentro del marco legal ecuatoriano[20].

Serrano-Picón y Vázquez-Calle argumentan que la actual definición de terrorismo en el COIP ecuatoriano presenta problemáticas y ambigüedades significativas, las cuales podrían afectar la efectividad de las medidas antiterroristas. Los autores destacan que estas ambigüedades permiten interpretaciones variadas y subjetivas al momento de clasificar un acto como terrorista, lo que podría obstaculizar la aplicación coherente de las leyes antiterroristas en Ecuador. Frente a esta situación, sugieren una reforma integral del artículo 366 del COIP, con el objetivo de precisar y limitar las conductas consideradas como ilícitas para enfrentar de manera más efectiva las amenazas terroristas modernas y dinámicas[21].

La Ley de Seguridad Pública y del Estado, promulgada el 9 de junio de 2014, proporciona el marco legal para la intervención de las Fuerzas Armadas en la lucha contra el terrorismo. Esta legislación permite que las Fuerzas Armadas apoyen, de manera complementaria, las tareas asignadas a la Policía Nacional para resguardar la seguridad interna y controlar el orden público. La colaboración coordinada entre estas instituciones es fundamental para la implementación de estrategias efectivas en respuesta a las amenazas terroristas, subrayando la importancia de una interpretación precisa y aplicación efectiva de las leyes para garantizar la eficacia de las operaciones conjuntas y contribuir significativamente a la seguridad nacional en el contexto de la lucha antiterrorista[22].

Las estrategias y medidas empleadas por las Fuerzas Armadas ecuatorianas en la lucha contra el terrorismo se enmarcan dentro de un contexto legal sólido, permitiendo la intervención militar en situaciones de grave conmoción interna. Estas acciones, que se respaldan en la declaración del estado de Excepción, la activación del Consejo de Seguridad Pública y del Estado (COSEPE) y las disposiciones gubernamentales para la intervención militar en actos terroristas, representan una convergencia compleja entre la seguridad nacional, los derechos humanos y el Estado de derecho.

3.5. El uso legal de la fuerza en operaciones contraterroristas y derechos humanos

La aplicación legal de la fuerza en contextos contraterroristas en Ecuador, y su relación con los derechos humanos, constituye un área que precisa de un análisis minucioso. La normativa ecuatoriana, específicamente la Ley Orgánica que Regula el Uso Legítimo de la Fuerza, provee un marco legal robusto que estipula la necesidad de equilibrar las exigencias operativas con el absoluto respeto a los derechos humanos. Este balance implica un entrenamiento exhaustivo y la implementación de protocolos detallados para asegurar que cualquier empleo de la fuerza,

---

20 ECUADOR. 2014. *Ley de Seguridad Pública y del Estado*. Quito: Registro Oficial, 9 junio 2014.

21 SERRANO-PICÓN, Paúl Andrés; VÁZQUEZ-CALLE, José Luis. El delito de terrorismo en Ecuador: Un estudio crítico. En: *Pol. Con. (Edición núm. 70) Vol. 7, No 5*, Mayo 2022, pp. 1687-1711. ISSN: 2550-682X.

22 ECUADOR. 2014. *Loc. Cit.*

particularmente la letal, se ejecute de manera gradual y únicamente en circunstancias donde alternativas menos drásticas sean ineficaces. Además, la ley enfatiza que dicha fuerza debe ser proporcional a la amenaza enfrentada, salvaguardando los derechos fundamentales en todo momento[23].

La mencionada ley es vital dentro del contexto de lucha antiterrorista, ya que delimita claramente los parámetros y condiciones bajo los cuales la fuerza pública, incluidas las Fuerzas Armadas, puede actuar frente a amenazas. Se destaca que las operaciones militares en estado de excepción deben someterse al liderazgo presidencial y complementar las funciones de la Policía Nacional en términos de orden público y seguridad ciudadana. Esto subraya la importancia de una actuación integrada y coordinada entre las diferentes agencias del Estado, subrayando que las Fuerzas Armadas actúan dentro de un marco de colaboración y no de manera unilateral,

Importante también es el mandato de la Ley Orgánica sobre el Uso Legítimo de la Fuerza que exige la fiscalización de las operaciones militares por parte de la Asamblea Nacional y la sociedad civil, promoviendo así la transparencia y la rendición de cuentas. Esta disposición refuerza la confianza en las intervenciones militares, asegurando que estas se realicen dentro de un contexto de legalidad y respeto por los derechos humanos.

En adición, la Ley Orgánica de Seguridad Pública y del Estado establece que la intervención de las Fuerzas Armadas en situaciones de emergencia debe estar siempre bajo la supervisión de autoridades civiles, manteniendo el respeto por los derechos humanos y libertades civiles, especialmente en operaciones antiterroristas. Esto refleja el compromiso del Ecuador con enfrentar desafíos de seguridad de manera que esté en consonancia con los principios democráticos y el respeto a los derechos fundamentales, alineándose con las directrices de la Estrategia Global contra el Terrorismo de la ONU, que enfatiza la importancia de adherirse al Estado de derecho y desarrollar sistemas de justicia penal efectivos.

3.6. Desarrollo de operaciones de contraterrorismo y antiterrorismo

Las operaciones militares contra organizaciones terroristas combinan tácticas represivas y ofensivas, orientadas a prevenir, anticipar y neutralizar actos terroristas. Estas estrategias buscan no solo detener a los actores terroristas directamente, sino también disminuir su influencia y desmantelar sus redes, constituyendo una amenaza a nivel regional y global. La lucha contra el terrorismo se fundamenta en medidas sostenibles y protectoras, enfocadas en la erradicación y en la necesidad de interactuar directamente para reprimir a estas organizaciones, subrayando la relevancia de una coordinación precisa y una comprensión profunda del entorno operativo[24].

Es esencial el apoyo y la colaboración de la sociedad en las operaciones de contraterrorismo. Las iniciativas antiterroristas resultan efectivas únicamente con la participación activa de la población, que debe ser liberada del control y la influencia de las fuerzas terroristas para garantizar el éxito de cualquier esfuerzo de apoyo. La liberación de la población bajo control

23 ECUADOR. 2022. *Loc. Cit*.

24 CALVILLO CISNEROS, José Miguel. 2023. "Los talibán 2.0: Del terrorismo al contraterrorismo" en *Studia Historica. Historia Contemporánea*, n.º 41, pp. 15-37. Disponible en: https://doi.org/10.14201/shhc2023411537. Este estudio examina la transformación de los Talibán y las implicaciones de este cambio para las estrategias de contraterrorismo y antiterrorismo, ofreciendo un marco para comprender la complejidad de la lucha contra el terrorismo en el actual contexto geopolítico.

terrorista es un paso crítico, ya que facilita las operaciones y fortalece la resistencia comunitaria contra las tácticas de terror.

El éxito en la lucha contra el terrorismo requiere de un compromiso constante a nivel global y regional, implicando a gobiernos y entidades especializadas en una colaboración estrecha para ubicar y neutralizar a las organizaciones terroristas y sus redes. Este esfuerzo coordinado busca incapacitar a dichos grupos para que no puedan utilizar el terrorismo como herramienta para alcanzar sus fines.

El fin de las operaciones de contraterrorismo es neutralizar la habilidad o voluntad de las organizaciones terroristas para conducir sus actos en contra de nuestro territorio, instalaciones críticas o intereses, debiendo emplear métodos como: la captura y neutralización del liderazgo terrorista y a sus subordinados claves, aislar a los terroristas de sus infraestructuras administrativa y logística, y desmantelar sus capacidades y bases. Para esto es menester la aplicación de todas las capacidades que dispone un gobierno junto con las de los países amigos, de manera simultánea, maniobrando de acuerdo a los niveles de la guerra para interrumpir, aislar y desmantelar a las organizaciones terroristas más peligrosas para la nación y donde la fuerza pública tiene que fortalecer los medios que le permitan influenciar en la población relevante e impactar en el ambiente operacional con capacidades multidominio que permitan accionar con otras fuerzas en:

- Asalto a instalaciones.
- Asalto a buses, vehículos, caravanas, etc.
- Asalto a aeronaves.
- Asalto a buques.

Estas misiones deben cumplirse mediante operaciones sorpresivas, con agilidad y una rápida penetración a la localización de un terrorista específico, con el propósito de neutralizar a militantes y líderes terroristas, obtener información, capturar o destruir su equipo, armamento e instalaciones, llevada a cabo en forma independiente o en apoyo a otra operación de contraterrorismo.

Para que el cumplimiento de una operación de contraterrorismo sea exitosa, no se debe dejar pasar por alto lo siguiente:

- La sorpresa.
- Productos de inteligencia detallados.
- Comunicaciones eficaces.
- La ejecución de la misión dentro de un mínimo de tiempo.
- La violencia de la acción en el objetivo.

3.7. Estrategias y tácticas de las Fuerzas Armadas del Ecuador en la lucha contra el terrorismo

Las estrategias y tácticas de las Fuerzas Armadas del Ecuador en la lucha contra el terrorismo reconocen que el terrorismo no se supera únicamente con la fuerza militar, las medidas de aplicación de la ley o las operaciones de inteligencia. La necesidad de abordar las condiciones que promueven la propagación del terrorismo es crucial, tal como lo resalta la Estrategia Global de las Naciones Unidas contra el Terrorismo. Esta estrategia subraya la importancia de enfrentar desafíos como la prevención de conflictos y la promoción del Estado de derecho, los derechos humanos, la buena gobernanza, la tolerancia y la inclusión para prevenir la radicalización que conduce a la violencia.

La Política de Defensa Nacional del Ecuador refuerza este enfoque, destacando la importancia crítica de una seguridad integral y la necesidad de un enfoque cohesivo en la seguridad nacional que une intereses y fortalece la cohesión social. Esta política subraya la planificación estratégica a largo plazo como esencial para abordar desafíos complejos de manera efectiva[25].

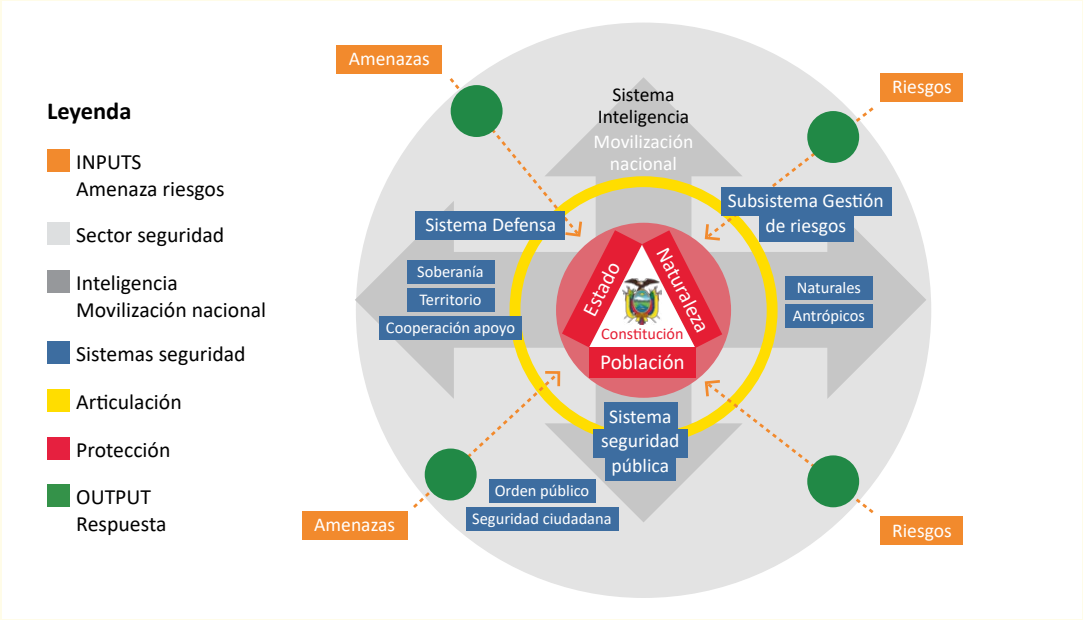
Las Fuerzas Armadas ecuatorianas aplican estrategias multidimensionales para debilitar los pilares de las organizaciones terroristas mientras fortalecen los de la sociedad ecuatoriana. Esto incluye la protección de la conexión con la población y el fortalecimiento de su capacidad de resistencia, al mismo tiempo que buscan socavar el liderazgo de los grupos terroristas. Reconocen la dificultad de lograr la destrucción militar total de organizaciones que se integran dentro de la población civil, priorizando estrategias que limiten su alcance operativo sin buscar su aniquilación absoluta.

Implementan tácticas que abarcan la disuasión, prevención y respuesta. Esto involucra desarrollar capacidades militares modernas para disuadir amenazas, promover la educación y la tolerancia para prevenir el terrorismo, y formar unidades especializadas como la Fuerza Contraterrorista del Ecuador, demostrando preparación y determinación para responder efectivamente ante ataques terroristas[26].

25 MINISTERIO DE DEFENSA NACIONAL. Política de Defensa Nacional del Ecuador 2018, pp. 22-24, 30-32, 45-47, 55-57. Quito: Ministerio de Defensa Nacional, 2018.

26 COMANDO CONJUNTO DE LAS FUERZAS ARMADAS. Manual militar de operaciones de Anti y Contraterrorismo. Quito: Comando Conjunto de las Fuerzas Armadas, 2020.

Figura N° 1
Articulación de actores para la planificación de operaciones



Fuente: Gabinete Sectorial de Seguridad[27]

3.7.1 Estrategias con agentes Nuclear, Biológico, Químico y Radiológico (NBQR), que deberían ser aplicadas por las Fuerzas Armadas ante atentados terroristas

Las nuevas amenazas híbridas conllevan a que las Fuerzas Armadas empleen estrategias que van fuera de una actuación convencional, permitiendo mantener la incertidumbre del adversario, bajo la presunción que estos grupos actúan sin una estructura organizada y con técnicas no habituales que difícilmente se pueden descifrar como en una tabla de ajedrez; es notorio, entonces, que las fuerzas legales deben entrenarse en aquellos escenarios que surgirían ante atentados terroristas, uno de estos es el actuar con agentes NBQR, que a más de ser disuasivos permitan accionar con la mínima letalidad cuando exista personas comunes que podrían estar afectados, siendo de gran importancia el conocimiento previo del personal militar en el uso de estos agentes químicos, los mismos que deben incluir lo siguiente:

a. *Desarrollo de Planes de emergencia claros:* Establecer y mantener planes de emergencia detallados para cada práctica NBQR, garantizando criterios claros para la preparación y respuesta ante cualquier emergencia que se presente.

b. *Optimización de estrategias de protección:* Implementar estrategias de protección de acuerdo con las normas de seguridad de la Organización para la Prohibición de

27 Modelo Sistémico de Seguridad en Plan Nacional de Seguridad Integral 2019-2030, coordinado por Grad. (S.P.) Francisco Drouet y desarrollado por el equipo interinstitucional bajo la dirección de Crnl. de E.M.C. Édison Mogollón y Crnl. de E.M.C. Amilcar Alvear. Quito: Ministerio de Defensa Nacional, 2019, p. 34.

Armas Químicas (OPAQ) y del Organismo Internacional de Energía Atómica (OIEA), priorizando la prevención y mitigación de riesgos en escenarios NBQR.

c. *Capacitación periódica del personal:* Impartir capacitaciones recurrentes y actualizadas sobre respuestas ante emergencias NBQR, fortaleciendo las habilidades del personal militar para enfrentar situaciones reales y que se conformen equipos de actuación sólidos donde cada uno identifique su rol de participación con sus responsabilidades dentro del grupo. Además, mantener una planificación constante que permita continuar la preparación de los miembros de las Fuerzas Armadas mediante talleres y capacitaciones, en estrecha colaboración con la Subsecretaría de Control y Aplicaciones Nucleares del Ecuador y el OIEA[28], así como la Organización para la Prohibición de Armas Químicas.

d. *Realización de ejercicios y evaluación continua:* Programar simulacros y ejercicios de verificación de preparación ante emergencias NBQR, evaluando los resultados para mejorar constantemente la capacidad de alistamiento y respuesta, adaptando de manera constante estrategias de actuación en equipos de trabajo establecidos.

e. *Definición de roles y responsabilidades:* Establecer claramente las funciones y responsabilidades de las instituciones del Estado, organizaciones internacionales y personal de respuesta en situaciones de emergencia NBQR.

f. *Planificación de capacitación conjunta:* Trabajar en coordinación con el Equipo Técnico de Armas Químicas del Ministerio de Defensa Nacional y la Subsecretaría de Control y Aplicaciones Nucleares del Ministerio de Energía y Minas para capacitar a las unidades de las Fuerzas Armadas en el manejo de emergencias NBQR de tal forma que pueda manejarse la integración en la planificación y ejecución de operaciones militares antiterroristas.

3.7.2. Estrategias de planificación y preparación

La organización y empleo de las Fuerzas Armadas en el Ecuador deben de manera obligatoria orientar estrategias a contrarrestar las amenazas, con prioridad en las zonas de frontera (que por su gran extensión, su permeabilidad es incontrolable), mediante un sistema integrado de alerta temprana articulado con el subsistema de inteligencia militar que le permita detectar oportunamente la inminencia de cualquier tipo de agresión, empleando comandos operacionales conformados por unidades del Ejército, Armada y Fuerza Aérea, con capacidad operativa y autonomía logística meritoria, mediante la preparación, prevención, disuasión defensiva, defensa y cooperación internacional, a fin de obtener la iniciativa y decisión estratégica, que permita alcanzar el objetivo político de la defensa en condiciones de empleo en el menor tiempo posible y con el mayor nivel de alistamiento operacional.

La planificación para hacer frente a esta amenaza se basa en implementar las estrategias que, como objetivo principal, recogen la acción de "neutralizar la amenaza que

28 ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA (OIEA). *Acerca del OIEA.* 2024. Disponible en: https://www.iaea.org/es/el-oiea [consulta: 14 de febrero de 2024]. El OIEA es el principal foro mundial intergubernamental para la cooperación científica y técnica en el ámbito nuclear, promoviendo el uso seguro, seguro y pacífico de la tecnología nuclear.

representa el terrorismo contra los ciudadanos y los intereses nacionales, dentro y fuera de las fronteras, reduciendo la vulnerabilidad de la sociedad y haciendo frente a los procesos de radicalización violenta". A su vez, para la consecución de este objetivo principal, la estrategia adoptada identifica cuatro objetivos específicos sobre los que sobresaldrá la acción del Estado; la prevención, protección, intervención y preparación.

Tabla N° 5
Líneas de acción para la planificación de operaciones militares contra el terrorismo

Línea de acción	Acciones
Prevención	• Reforzar los mecanismos establecidos en materia de lucha contra la financiación del terrorismo. • Reforzar la contribución del Ecuador en la lucha contra el terrorismo a nivel internacional en las organizaciones a las que pertenece, en especial en la OEA, ONU y OMI y en aquellas iniciativas de las que forma parte. • Reforzar el testimonio de las víctimas del terrorismo como la mejor vía de contrarrestar la narrativa terrorista. • Fomentar el diálogo intercultural e interreligioso.
Protección	• Robustecer las capacidades nacionales de lucha contra el terrorismo y la cooperación y coordinación de esfuerzos contra el terrorismo entre los distintos organismos implicados a nivel nacional. • Cooperar con los países socios más afectados por el terrorismo y adoptar medidas de mejora en el control de fronteras.
Intervención	• Mejorar las capacidades de investigación e inteligencia, asegurar el desarrollo tecnológico de los servicios de inteligencia e información para hacer frente al uso intensivo de las nuevas tecnologías por parte de los grupos terroristas e impedir el acceso a las capacidades y materiales necesarios para acometer atentados. • Reforzar los instrumentos legales en la lucha contra el terrorismo
Preparación	• Robustecer la adopción de las medidas y planes necesarios que aseguren la sinergia y coordinación de todos los organismos con responsabilidad en la materia en caso de atentado terrorista. • Minimizar las consecuencias y dar apoyo inmediato y permanente a las víctimas de ataques terroristas.

Fuente: Manual Militar de Operaciones de Antiterrorismo y Contraterrorismo (2023)[29]

29 LUNA QUIROZ, Marlon, director. *Manual militar de operaciones de anti y contraterrorismo*, 2ª ed. Quito: Ministerio de Defensa Nacional, Dirección de Educación del Ejército, 2023, [en línea]. Disponible en: https://portal.ejercito.mil.ec/Menu/ingresaSistema.do?mcnvbdfh2342kjlkjM=D2441975FFD3840E&dgdfgdDFg354SDFSssssdf=7344D4D97B704C9D&xcodkdyd502Yreetrlpdjgd=E9764EDA2222BF0E. [Consulta: 14 de febrero de 2024].

3.7.2.1 Acciones para la planificación de operaciones militares contra el terrorismo basadas en las líneas de acción

a. Prevención

Mientras que la prevención total de actos terroristas es casi imposible, la eliminación de las causas que los terroristas explotan puede ser el factor más importante en la prevención del terrorismo. Con frecuencia, las causas del desorden público vienen de la corrupción política, la discriminación social, la privación económica, las diferencias ideológicas, las diferencias religiosas y las influencias extranjeras. Todas estas causas ayudan en el desarrollo de la violencia y actividades terroristas. La eliminación de estos problemas puede requerir la intervención del gobierno. De esta manera, el gobierno contrarresta y evita la expansión terrorista.

Un programa efectivo de contraterrorismo activa las acciones de prevención, esto depende de la identificación oportuna de problemas los cuales pueden desarrollarse en violencia y confrontaciones. Indicadores producidos de los análisis de pasados incidentes terroristas son valiosos instrumentos en el análisis de la amenaza y en la estimación de inteligencia. En muchos casos estos indicadores pueden aparecer como el ejercicio normal de los derechos democráticos. También se debe conocer que muchos terroristas son bien entrenados en la subversión del proceso democrático y usan el sistema para adelantar sus causas de lucha y esta manipulación termina, por lo general, con la destrucción del sistema democrático.

b. Protección

Entrenar fuerzas especiales preparadas para contrarrestar tácticas terroristas, con la habilidad de impedir ataques, aprehender terroristas o reaccionar con rapidez ante un incidente terrorista, permiten accionar con efectividad, pero no tendrá un efecto exitoso sin el aporte de operaciones de inteligencia efectivas. Para asegurar la protección deben articularse los siguientes aspectos:

1) Inteligencia.

2) Análisis de la amenaza.

3) Seguridad física.

4) Seguridad personal.

5) Seguridad operacional.

6) Autoridad y jurisdicción.

7) Manejo de crisis.

c. Intervención

La intervención táctica se ejecutará para dar una adecuada respuesta a una crisis de rehenes con presencia terrorista donde se pongan en riesgo los intereses nacionales, para

lo cual se deben maniobrar con técnicas determinadas por fases que permitan evaluar las operaciones y accionar en forma sincronizada:

1) Fase I

a) Acción local.

b) Reporte del incidente.

c) Acción policial local.

d) Aislar, contener, evacuar civiles y personal local.

e) Recopilar información adicional.

f) Determinar el motivo del acto terrorista.

g) Notificar a la autoridad competente.

2. Fase II

a) Acción policial especializada.

b) Acción militar local.

c) Evaluación de crisis.

3. Fase III

a) Acción integral nacional.

b) Empleo unidad militar contraterrorista.

d. Preparación

En esta fase radica la importancia de identificar los objetivos de los grupos terroristas, destacando que el objetivo final puede ser la intimidación o el derrocamiento del gobierno de turno para la imposición de sus propios intereses mediante la aplicación de la violencia y la amenaza. El contar con unidades especializadas, bien entrenadas y equipadas, para proveer una respuesta táctica a estos incidentes permitirá actuar militarmente de manera eficiente dentro de un marco legal, bajo un fuerte control del gobierno cuando así se lo determine. Si bien una respuesta mediante la intervención táctica es una necesidad en algunos casos, el carácter de esta respuesta tiene que ser basada en el tipo de acción terrorista.

3.7.3. Cooperación interinstitucional nacional e internacional

La gobernanza en temas de seguridad representa un pilar fundamental en la estrategia antiterrorista de las Fuerzas Armadas ecuatorianas. Estas trabajan de manera estrecha y coordinada con diversas instituciones del Estado, siendo la Policía Nacional, el Ministerio del Interior y el Ministerio de Justicia actores clave en esta colaboración. Esta estrecha relación se basa en la complementariedad de habilidades y recursos que cada entidad aporta para afrontar eficazmente la amenaza terrorista. La Policía Nacional, en sus competencias, brinda conocimiento detallado sobre la situación interna del país, apoyo en operaciones

urbanas y manejo directo en la prevención del delito, mientras que el Ministerio de Justicia proporciona un marco legal y jurídico sólido para respaldar las acciones antiterroristas[30].

La cooperación a nivel nacional se amplía a un esfuerzo conjunto en el ámbito internacional, permitiendo a las Fuerzas Armadas ecuatorianas desarrollar tácticas más efectivas mediante la mejora de la inteligencia, la movilidad, la capacitación y el equipamiento. Este enfoque coordinado ha demostrado ser fundamental para la efectividad de las operaciones antiterroristas[31].

A nivel internacional, Ecuador se integra activamente en mecanismos de cooperación regional e internacional, destacándose su participación en la Organización del Tratado de Cooperación Amazónica (OTCA). Esta participación fomenta el intercambio de información y mejores prácticas con países vecinos como Colombia y Perú, facilitando un enfoque colaborativo hacia los desafíos transfronterizos del terrorismo. La vinculación con organismos internacionales, como la Organización de las Naciones Unidas (ONU) y la Organización de Estados Americanos (OEA), fortalece las capacidades de Ecuador en contraterrorismo mediante capacitación, asesoramiento y apoyo.

Los acuerdos de cooperación bilateral con países líderes en la lucha contra el terrorismo, incluidos Estados Unidos y España, permiten a las Fuerzas Armadas Ecuatorianas acceder a tecnología avanzada, intercambiar inteligencia y participar en entrenamientos conjuntos, mejorando su preparación para enfrentar un conflicto asimétrico[32].

Esta sinergia entre las Fuerzas Armadas y las estructuras de gobernanza tanto nacional como internacional promueve una respuesta integral y coordinada ante las amenazas terroristas. La cooperación se manifiesta en un intercambio constante de información, estrategias conjuntas y acciones coordinadas que no solo optimizan recursos y maximizan el impacto de la lucha contra el terrorismo, sino que también fortalecen la confianza social en las instituciones encargadas de la seguridad nacional.

IV. CONCLUSIONES

Desde un punto teórico, la amenaza terrorista puede requerir de una respuesta militar, lo cual siendo discutible dependerá de cada país; su base legal generada a través de varios acuerdos permiten hacerlo en el contexto ecuatoriano, donde la necesidad de una respuesta robusta y coordinada para preservar el Estado de derecho y proteger a la población civil de la violencia criminal se hace imperante. En el ámbito práctico, las actuaciones de las fuerzas responsables de hacer cumplir la ley tienen implicaciones significativas para la seguridad nacional, donde la capacitación, el entrenamiento, las alianzas estratégicas en seguridad y el soporte logístico preciso, conforman una sinergia que permiten cumplir los objetivos de

30 ROA, S.; PAZ Y MIÑO, E. (2023). "La declaratoria de terrorismo como amenaza en Ecuador, explicada". *GK*. Disponible en: https://gk.city/2023/05/04/declaratoria-terrorismo-amenaza-ecuador-explicada/ [consulta: 14 de febrero de 2024].

31 ARÁUZ, M., & CEVALLOS, J. (2021). Capacidades militares y respuesta al terrorismo en Ecuador. *Revista de Estudios de Seguridad y Defensa*, 12(3), 45-62. https://doi.org/10.24215/23142766e021

32 VILLACÍS, J., & TRUJILLO, M. (2018). Cooperación bilateral en materia de contraterrorismo: la alianza entre Ecuador y Estados Unidos. *Revista Española de Estudios Internacionales*, 15(1), 67-84. https://doi.org/10.24215/23142766e015

seguridad nacional y con esto asegurar una economía en progreso que se desarrolle en un ambiente de paz y de inversión para el fortalecimiento de la seguridad en Ecuador.

Aunque el Ecuador ha experimentado un nivel relativamente bajo de terrorismo en comparación con otros países, es fundamental mantener una vigilancia constante y fortalecer las medidas de seguridad para prevenir y responder eficazmente a los actos terroristas con la intervención de Fuerzas Contra Terroristas mediante técnicas, tácticas y procedimientos en forma eficaz y eficiente, teniendo siempre presente el grave problema de los posibles daños colaterales, donde además la cooperación internacional y el intercambio de información seguirán siendo elementos clave para combatir el terrorismo tanto en Ecuador como en todo el mundo.

Estas tácticas de conflicto asimétrico permitirán fortalecer la capacidad de defensa mediante la implementación de estrategias en inteligencia, vigilancia y reconocimiento para identificar y neutralizar posibles amenazas, donde la capacidad, capacitación y equipamiento para llevar a cabo operaciones de seguimiento y vigilancia resulta decisivo para prevenir ataques y desmantelar células terroristas, ofreciendo una respuesta efectiva, contundente y con rapidez en la toma de decisiones que permitan adaptarse a diferentes escenarios, brindando a las Fuerzas Armadas una ventaja en su combate para desarticular cualquier organización de este tipo.

REFERENCIAS BIBLIOGRÁFICAS

ARÁUZ, M., & CEVALLOS, J. (2021). Capacidades militares y respuesta al terrorismo en Ecuador. *Revista de Estudios de Seguridad y Defensa*, 12(3), 45-62. https://doi.org/10.24215/23142766e021

BANCO MUNDIAL. Ecuador: panorama general [en línea]. [Fecha de consulta: 2 abril 2024]. Disponible en: https://www.bancomundial.org/es/country/ecuador/overview

CARRASCO, J. y PILALUMBO, W. (2022). *Guerra de cuarta generación en la frontera norte ecuatoriana*. Revista de la Academia de Guerra del Ejército Ecuatoriano, vol. 15, no. 1, pp. 13-13. ISSN 26005697. DOI 10.24133/AGE.N15.2022.07.

COMANDO CONJUNTO DE LAS FUERZAS ARMADAS DEL ECUADOR. 2022. Operaciones y resultados durante la vigencia del Decreto Ejecutivo 411. En: *Informe de Gestión 2022: Resultados en las operaciones - Dirección de Operaciones del CC.FF.AA*. Quito: Comando Conjunto de las Fuerzas Armadas del Ecuador.

COMANDO CONJUNTO DE LAS FUERZAS ARMADAS. (2022). *Plan Estratégico Institucional 2021-2025*. Quito: Comando Conjunto de las Fuerzas Armadas del Ecuador.

COMANDO CONJUNTO DE LAS FUERZAS ARMADAS. Manual militar de operaciones de Anti y Contraterrorismo. Quito: Comando Conjunto de las Fuerzas Armadas, 2020.

COMITÉ INTERNACIONAL DE LA CRUZ ROJA. Protocolo adicional a los Convenios de Ginebra de 1949 relativo a la protección de las víctimas de los conflictos armados internacionales (Protocolo I). Ginebra: CICR, 1977.

CRONIN, Audrey Kurth. How al-Qaeda ends: the decline and demise of terrorist groups. International Security. 2006, vol. 31, no. 1, pp. 7-48. ISSN 0162-2889.

ECUADOR. 2008. *Constitución de la República del Ecuador*, Artículo 158. Quito: Registro Oficial, 20 octubre 2008.

ECUADOR. 2014. *Ley de Seguridad Pública y del Estado*. Quito: Registro Oficial, 9 junio 2014.

ECUADOR. Ministerio de Defensa Nacional. *Plan Nacional de Seguridad Integral 2019-2030*. Quito, 2019. Coordinación por Grad. (S.P.) Francisco Drouet. Director de proyecto Crnl. de E.M.C. Édison Mogollón y Crnl. de E.M.C. Amilcar Alvear.

ESTADO MAYOR CONJUNTO DE LAS FUERZAS ARMADAS DEL ECUADOR. Plan Estratégico Institucional de FF.AA. 2021-2033. Quito, 2021.

GRIES, Thomas y REDLIN, Maiken. Las raíces del terrorismo: una investigación cuantitativa sobre las causas socioeconómicas de la actividad terrorista. Revista de Política y Gobierno. 2019. Vol. 26, no. 1, pp. 59-81. ISSN 1665-2037.

HOFFMAN, Bruce. Inside terrorism. New York: Columbia University Press, 2006. 456 p. ISBN 978-0-231-12699-9.

LUNA QUIROZ, Marlon, director. Manual militar de operaciones de anti y contraterrorismo. 2ª ed. Quito: Ministerio de Defensa Nacional, Dirección de Educación del Ejército, 2023. Disponible en: https://portal.ejercito.mil.ec/Menu/ingresaSistema.do?mcnvb-dfh2342kjlkjM=D2441975FFD3840E&dgdfgdDFg354SDFSssssdf=7344D4D97B704C-9D&xcodkdyd502Yreetrlpdjgd=E9764EDA2222BF0E. [Consulta: 14 de febrero de 2024].

MARTÍNEZ Muñoz, Pablo. Las fuerzas armadas de Ecuador y su rol en la lucha contra el crimen organizado transnacional. Revista Científica General José María Córdova. 2017. Vol. 15, no. 20, pp. 67-88. ISSN 1900-6586.

MINISTERIO DE DEFENSA NACIONAL. (2023). *Informe de Gestión CCFFAA*. Quito: Ministerio de Defensa Nacional.

MINISTERIO DE DEFENSA NACIONAL. 2018. Política de Defensa Nacional del Ecuador. Quito: Ministerio de Defensa Nacional. Disponible en formato PDF.

NACIONES UNIDAS. 2024. *Estrategia Global de las Naciones Unidas contra el Terrorismo*. [en línea] Disponible en: https://www.un.org/counterterrorism/es/un-global-counter-terrorism-strategy [Consulta: 14 febrero 2024].

NOBOA AZÍN, Daniel. (2024). *Decreto Ejecutivo No. 111*. Quito: Presidencia de la República del Ecuador.

REPÚBLICA DEL ECUADOR. 2022a. Decreto Ejecutivo 411, 30 de abril de 2022. Se declara el estado de excepción por grave conmoción interna por razones de seguridad ciudadana en las provincias de Guayas, Esmeraldas y Manabí. Quito: Registro Oficial.

REPÚBLICA DEL ECUADOR. 2022b. Decreto Ejecutivo 527 y 561, 14 de agosto de 2022. Se declara el estado de excepción en el Distrito Metropolitano de Guayaquil, Durán, Samborondón y Guayaquil, por incremento de actividades delictivas. Quito: Registro Oficial.

REPÚBLICA DEL ECUADOR. 2022c. Decreto Ejecutivo 588 y 589, 01 y 04 de noviembre de 2022. Se declara el estado de excepción en las provincias de Guayas, Esmeraldas y Santo Domingo por homicidios, asesinatos y sicariatos. Quito: Registro Oficial.

SERRANO-PICÓN, Paúl Andrés; VÁZQUEZ-CALLE, José Luis. El delito de terrorismo en Ecuador: Un estudio crítico. En: *Pol. Con. (Edición núm. 70) Vol. 7, No 5*, Mayo 2022, pp. 1687-1711. ISSN: 2550-682X.

STERN, Jessica. Terror in the name of God: why religious militants kill. New York: Ecco, 2003. 352 p. ISBN 978-0-06-050528-8.

VILLACÍS, J., & TRUJILLO, M. (2018). Cooperación bilateral en materia de contraterrorismo: la alianza entre Ecuador y Estados Unidos. *Revista Española de Estudios Internacionales*, 15(1), 67-84. https://doi.org/10.24215/23142766e015

WEBER, Max. Economía y sociedad: esbozo de sociología comprensiva. México D.F.: Fondo de Cultura Económica, 2014. 1245p. ISBN 978-84-375-0728-7.

WEBER, Max. La política como vocación. Madrid: Alianza Editorial, 2009. 188p. ISBN 978-84-206-6061-0.

LA INTELIGENCIA CRIMINAL: CONCEPTO, IMPLEMENTACIÓN, EXPERIENCIAS COMPARADAS∞

JOSÉ MANUEL UGARTE•

RESUMEN

La inteligencia criminal es conocimiento sobre el delito, para prevenirlo, y enfrentarlo con eficacia. En diversos países del mundo para obtener, elaborar y difundir ese conocimiento se crean organismos de inteligencia criminal, constituidos fundamentalmente por policías, por analistas profesionales en diversas disciplinas para comprender e interpretar al delito, por técnicos informáticos y personal administrativo de apoyo, y se constituyen órganos de inteligencia criminal en las instituciones policiales, fuerzas de seguridad, y otros órganos que participan de la seguridad pública, interconectándose telemáticamente con el organismo de inteligencia criminal cabeza del sistema, trabajando todos de acuerdo con una doctrina común. Existen otras formas organizativas con una finalidad similar: la de conocer al delito, la de interpretar el ambiente criminal (Ratcliffe) que es lo que es preciso lograr.

Palabras clave: Inteligencia criminal; delito organizado; doctrina; interconexión; sistema.

CRIMINAL INTELLIGENCE: CONCEPT, IMPLEMENTATION, COMPARED EXPERIENCES.

ABSTRACT

Criminal intelligence is knowledge about crime, to prevent it, and confront it effectively. In various countries around the world to obtain, develop, and disseminate this knowledge, criminal intelligence organizations are created, consisting mainly of police officers, professional analysts in various disciplines to understand and interpret crime, computer technicians and administrative support staff, and criminal intelligence units are established in police institutions, security forces, and other bodies that participate in public security, interconnecting

• Doctor de la Universidad de Buenos Aires (área Derecho Administrativo), abogado y especialista en Derecho Administrativo y Administración Pública por la referida Universidad, en la que es profesor en grado y postgrado. Es además profesor en la Maestría en Derecho Administrativo de la Universidad Abierta Interamericana y en la Maestría en Seguridad Pública de la Universidad del Gran Rosario. manuguart@gmail.com ORCID: https://orcid.org/0000-0003-3300-4529

∞ Fecha de recepción: 230424 - Fecha de aceptación: 260624.

telematically with the head criminal intelligence body of the system, all working by accordance with a common doctrine. There are other organizational forms with a similar purpose: that of knowing crime, that of interpreting the criminal environment (Ratcliffe), which is what must be achieve

Key words: Criminal intelligence; organized crime; doctrine; interconnection; system.

INTELIGÊNCIA CRIMINAL: CONCEITO, IMPLEMENTAÇÃO, EXPERIÊNCIAS COMPARADAS

RESUMO

A inteligência criminal é o conhecimento sobre o crime, para preveni-lo e enfrentá-lo de forma eficaz. Em vários países do mundo, para obter, desenvolver e difundir este conhecimento, são criadas organizações de inteligência criminal, constituídas principalmente por policiais, analistas profissionais em diversas disciplinas para compreender e interpretar o crime, técnicos de informática e pessoal de apoio administrativo, e inteligência criminal órgãos das instituições policiais, forças de segurança e outros órgãos que participam na segurança pública, interligando-se telematicamente com o órgão responsável pela inteligência criminal do sistema, todos trabalhando de acordo com uma doutrina comum. Existem outras formas organizacionais com finalidade semelhante: a de conhecer o crime, a de interpretar o ambiente criminoso (Ratcliffe), que é o que deve ser alcançado.

Palavras-chave: Inteligência criminal; crime organizado; doutrina; interligação; sistema.

1. ¿Qué es la inteligencia criminal?

Inteligencia criminal es, básicamente, inteligencia sobre el delito. Es conocimiento, información elaborada, utilizando técnicas de análisis, sobre el delito: quiénes lo cometen, cómo, dónde, cuándo, con qué, con quién(es), a quién (es) –incluyendo el conocimiento o estudio de los delincuentes y de las víctimas– por qué, para qué, etc., con la finalidad de orientar la prevención del delito y también la investigación criminal. Conocer al delito es la mejor forma de prevenirlo y también de enfrentarlo.

En sentido amplio, hacen inteligencia criminal los fiscales, los jueces, los abogados, los policías, los periodistas especializados, todas las personas e instituciones relacionadas con la justicia criminal. Pero de ese amplio universo, habremos de escoger una parte.

Habremos aquí de referirnos a la actividad de inteligencia sobre el delito realizada por los organismos de inteligencia criminal y por las policías y fuerzas de seguridad

Como Monsieur Jourdain de Molière, que hacía prosa sin saberlo, todo policía siempre hizo inteligencia criminal años antes de que esta actividad se conociera con tal.

Siempre fue frecuente en las instituciones policiales incrementar las capacidades resultantes de la memoria y de la experiencia policial con sistemas de archivos, manejados por personal idóneo –así, el antiguo *collator* de instituciones policiales anglosajonas–.

Pero el crecimiento tecnológico y organizativo del delito, estructurado en organizaciones criminales con importantes recursos técnicos y financieros, poder corruptor sobre la política y la administración pública, sobre jueces, fiscales, e incluso la propia policía, capacidad para actuar en diversas jurisdicciones e incluso en múltiples países, dio lugar a la necesidad de una respuesta equivalente.

Surgió así la inteligencia criminal, capacidad organizada y específica de obtención de información y de análisis del Estado, para conocer a fondo al delito y permitir la elaboración de una respuesta equivalente o superadora de la amenaza.

Tiende a ser una actividad organizada a nivel ministerial de los Estados, y realizada tanto a nivel del Estado Nacional como bajo orientación y dirección nacional, a nivel de jurisdicciones locales y municipales, actuando base a una doctrina –conjunto de normas y procedimientos– común a todos los participantes, interconectando telemáticamente a todos los actores de la seguridad pública, desarrollando capacidades de análisis tanto en organismos específicos de inteligencia criminal, en aquellos países que cuentan con ellos, como en las instituciones policiales, fuerzas de seguridad, e incluso en otras instituciones vinculadas a la seguridad pública, particularmente las instituciones penitenciarias, Aduanas, Impuestos, etc.

La inteligencia criminal se presta especialmente a la cooperación internacional, dado que a diferencia de la actividad de inteligencia de Estado y de la inteligencia militar, no involucra las fuentes, métodos y operaciones particularmente sensibles que caracterizan a estos tipos y estructuras de inteligencia.

La inteligencia criminal suele organizarse a nivel regional, como ha sucedido en la Unión Europea con EUROPOL, auténtico organismo de inteligencia criminal regional, y a nivel internacional con INTERPOL – Organización Internacional de Policía Criminal.

En América Latina, entre varias tentativas realizadas a nivel subregional, encontramos la Comunidad de Policías de América (AMERIPOL), organización formada por instituciones policiales y fuerzas de seguridad de múltiples países latinoamericanos, con apoyo estadounidense y europeo, que ha dado motivo a la suscripción, el 9 de noviembre de 2023, del Tratado de Brasilia entre 13 de los países cuyas instituciones policiales y de seguridad integraban AMERIPOL, otorgando personería jurídica internacional al ente y estableciendo normas institucionales básicas.

En definitiva, la inteligencia criminal, tal como ha sido desarrollada en buena parte del mundo, destacándose la Organización Internacional de Policía Criminal (INTERPOL), la Oficina Europea de Policía (EUROPOL) y, como organismos específicos, la National Crime

Agency (Agencia Nacional contra el Delito) del Reino Unido, la Australian Criminal Intelligence Commission (Comisión Australiana contra el delito); el Servicio Nacional de Inteligencia Policial del Reino de Holanda (IPOL), el Servicio de Inteligencia Criminal de Austria, y la Agencia sobre Delito Organizado y Financiero de la Policía de Nueva Zelandia –entre otros casos– constituye, antes que nada, parte de la función de seguridad pública, ejercida fundamentalmente (aunque no exclusivamente) por policías, frecuentemente con la cooperación de personal de analistas y de apoyo sin estado policial.

Definiremos la inteligencia criminal como la aplicación de la metodología propia de la actividad de inteligencia, fundamentalmente en materia de análisis, a la actividad de seguridad pública y policial.

Ello así, tanto:

a) En el nivel estratégico: determinación de situación en materia de seguridad pública, de todo el país, o de una región o área determinada, o circunscripta a determinado o determinados delitos, comprendiendo su probable evolución, amenazas, tendencias y causas a corto, mediano y largo plazo, destinada a orientar a la política de seguridad pública del país, o de una región o área determinada, o respecto de determinado delito;

b) En el nivel operacional: conocimiento destinado a guiar a jefes policiales, generalmente de rango medio, a establecer prioridades en su accionar, a emplear con mayor eficiencia y eficacia recursos escasos, a efectuar un despliegue eficaz, a emplear tácticas adecuadas, a fin de obtener mayores resultados en materia de reducción del delito;

c) En el nivel táctico: conocimiento de las organizaciones criminales –campo fundamental de interés de la inteligencia criminal– y de aquellas formas delictivas que por su complejidad, gravedad, reiteración y consecuencias, no logran ser prevenidas eficazmente por la investigación policial, fiscal o judicial del caso individual.

Se ha definido a la inteligencia criminal de un modo más general como …la creación de un producto de conocimiento de inteligencia que apoya la toma de decisiones en las áreas de accionar policial, reducción del delito, y prevención del delito……[1].

Otros autores definen a la inteligencia criminal como …un proceso que involucra planeamiento y dirección, recolección, evaluación, cotejo, análisis, diseminación y ree-evaluación de información sobre sospechosos criminales y/u organizaciones…[2].

1 RATCLIFFE, Jerry H. Integrated Intelligence and Crime Analysis: Enhanced Information Management for Law Enforcement Leaders, Second Edition, COPS-Police Foundation, Washington, 2007.

2 HARRIS, Don. Basic Elements of Intelligence. Revised. Law Enforcement Assistance Administration September, Washington D.C., 1976, pp. 1.8. Citado por MOREHOUSE, Bob. The Role of Criminal intelligence in Law Enforcement en MOREHOUSE Bob, PETERSON, Marilyn B. y PALMIERI, Lisa. (Eds.). Criminal Intelligence for the 21st century, Law Enforcement Intelligence Units (LEIU) & International Association of Law Enforcement Intelligence Analysts (IALEIA), Sacramento & Richmond, reimpresión, 2017.

La inteligencia criminal provee conocimiento que permite a las autoridades policiales establecer una respuesta proactiva al delito[3]. Ella permite a las agencias policiales identificar y entender a los grupos criminales que están operando en sus áreas. Una vez que los grupos criminales son identificados y sus hábitos conocidos, las autoridades policiales pueden comenzar a evaluar las actuales tendencias en el delito y anticipar, y posiblemente prevenir, futuras actividades criminales. La inteligencia criminal también provee el conocimiento en el cual basar decisiones y elegir blancos apropiados (sujetos, grupos criminales, o negocios) para investigaciones. Aunque la inteligencia criminal puede ser utilizada para asistir en investigaciones, operaciones de vigilancia y la prosecución de casos, también provee a las agencias policiales la capacidad de manejar eficazmente recursos, presupuestos, y cumplir su responsabilidad en anticipar amenazas a la comunidad para prevenir el delito…[4].

Uno de sus cultores más destacados, Jerry Ratcliffe, antiguo policía inglés, hoy profesor y académico, fue uno de los fundadores e impulsores de lo que pasó a constituir uno de los modos fundamentales de entender el accionar policial: la concepción sobre el modo de accionar en seguridad pública conocido como intelligence-led policing (accionar policial guiado por la inteligencia) que destacó el rol fundamental de la inteligencia criminal para obtener un accionar policial llevado a cabo sobre la base del conocimiento, sustituyendo a la intuición o a la improvisación, destacando el rol fundamental de la inteligencia criminal para fundamentar políticas y estrategias en seguridad pública formuladas sobre la base del conocimiento, así como un accionar táctico eficaz en dicha materia, también guiado por la inteligencia criminal.

2. Inteligencia criminal: distinciones necesarias

2.1 Inteligencia criminal e investigación criminal

La inteligencia criminal constituye conocimiento sobre el delito, para orientar la política de seguridad pública en todos sus niveles, incluyendo las policías, rigiéndose en aquellos países en los que alcanzó mayor desarrollo, por leyes y normas específicas, y en los países latinoamericanos, por las normas que rigen la actividad de inteligencia.

Tiene por destinatarios y está fundamentalmente dirigida por funcionarios del órgano ejecutivo y/o por policías.

Siendo la función de la actividad de inteligencia criminal la producción de conocimiento sobre el delito, no produce pruebas para el proceso penal, ni se vincula con jueces, salvo para alguna cooperación que le sea solicitada a través del órgano ejecutivo.

Es realizada por organismos de inteligencia criminal constituidos por policías o por policías y por analistas de inteligencia criminal, o bien por órganos de inteligencia criminal formados dentro de las instituciones policiales y fuerzas de seguridad.

---

3 AUMOND, Karen. Tactical and Strategic Intelligence. Issues of Interest to Law Enforcement. Criminal Intelligence. A Vital Police Function. Law Enforcement Intelligence Unit (LEIU), February 1998, pp. 35-36. Citado por MOREHOUSE, Bob. The Role of Criminal intelligence in Law Enforcement en MOREHOUSE, Bob. "et al". Ibíd

4 MOREHOUSE Bob. The Role of Criminal intelligence in Law Enforcement, en MOREHOUSE, Bob. et al. Ibid.

La investigación criminal consiste en la determinación relativa si un delito ha sido o no cometido, y en caso afirmativo, su esclarecimiento, la individualización de sus autores, y la obtención de pruebas válidas para el proceso penal.

Es protagonizada, en países con régimen procesal penal acusatorio, por fiscales y por policías, y en países con régimen penal inquisitivo, por jueces de instrucción y por policías.

Se rige por las normas en materia procesal penal, y está bajo el control del juez y del fiscal.

Se caracteriza por el caso penal –investigación de un delito o delitos determinados– que marca sus límites.

Desde el punto de vista policial, caracteriza a esta función la cooperación con el órgano judicial para el proceso penal, que incluye la obtención de pruebas procesalmente válidas.

Se debe señalar, no obstante, que en la actualidad organismos de inteligencia criminal como la National Crime Agency (NCA) (Agencia sobre el Delito) británica, la Australian Criminal Intelligence Commission (ACIC) (Comisión Australiana de Inteligencia Criminal), entre otros, realizan también investigación criminal en casos importantes de delito organizado.

2.2 La inteligencia criminal, la inteligencia nacional, la inteligencia de seguridad, y la inteligencia militar

Mientras que la inteligencia criminal es parte de la función de seguridad pública y, especialmente, de la función policial, la inteligencia nacional constituye parte de la función de seguridad del Estado, y la inteligencia militar, de la función de defensa nacional.

Dentro de la inteligencia nacional, el concepto de inteligencia de seguridad (security intelligence) hace referencia a la obtención de información y la elaboración de inteligencia con relación a las amenazas contra la seguridad del Estado derivadas del accionar de potencias extranjeras dentro del propio país y contra sus intereses –espionaje, sabotaje, operaciones encubiertas– así como sobre aquellas amenazas originadas dentro del propio país, con o sin apoyo externo, con el objeto de, empleando métodos ilegales, cambiar las autoridades, afectar o limitar seriamente el desempeño de aquéllas, o atentar contra el sistema democrático, o bien el accionar de organizaciones que pretenden imponer sus ideas políticas, económicas y sociales a través de la violencia o la intimidación –según los casos, subversión o terrorismo-.

La inteligencia en estos supuestos suele estar a cargo de organismos de inteligencia de seguridad. Es el caso, entre muchos otros, del Servicio de Seguridad del Reino Unido, del Servicio Canadiense de Inteligencia de Seguridad, de la Organización Australiana de Inteligencia de Seguridad, de la Oficina Federal de Defensa de la Constitución (VfB) alemana y de sus similares en los Lander o estados locales de la República Federal de Alemania.

Dichos organismos no producen inteligencia criminal, ni se confunden con ella.

En Estados Unidos de América, esta función está a cargo de la Oficina Federal de Investigación, que conforme a la Directiva del Procurador General sobre Operaciones Do-

mésticas del FBI, es tanto una agencia federal de investigación como una agencia de inteligencia. Asimismo, en Francia la Dirección General de Seguridad Interior, organismo de naturaleza policial, ejerce dentro del país la aludida función, sin dejar de constituir un organismo de policía judicial.

En cuanto a la inteligencia criminal, como ha sido señalado, esta función está a cargo de organismos de inteligencia criminal integrados mayormente por policías y por analistas sin estado policial, o bien fundamentalmente por policías; si bien en casos como el Reino Unido, como veremos, esa integración es hoy más variada.

La característica fundamental de la inteligencia criminal es la de tener como objeto el delito. A diferencia tanto de la inteligencia nacional como de la inteligencia militar, su objeto no está constituido por las actividades políticas, militares, diplomáticas y de inteligencia de otros países, ni sus intenciones en materia política, económica o militar.

Cabe destacar que mientras la inteligencia nacional suele estar protagonizada por agentes de inteligencia, que frecuentemente tienen identidad secreta, y que está caracterizada, al igual que la inteligencia militar, por un particular rigor en cuanto al secreto sobre identidades, fuentes, métodos y operaciones, así como por prácticas de compartimentación, tales prácticas tienen un rigor mucho menor o frecuentemente no existen en inteligencia criminal.

2.3. Inteligencia criminal y análisis del delito.

El análisis del delito (crime analysis) consiste en la recolección y el análisis de datos relativos a delitos cometidos –fundamentalmente utilizando formularios uniformes y adecuadamente diseñados de informe policial sobre hechos delictivos–[5], unidos a datos obtenidos en investigaciones criminales, causas judiciales, informantes u otros medios, así como datos sociológicos, económicos y geográficos, entre otros adecuadamente guardados en bases de datos relacionales con auxilio de sistemas informáticos especialmente diseñados.

Sobre tales bases, se realiza análisis de carácter espacial –empleando sistemas informáticos georeferenciados de diverso grado de complejidad, para determinar la localización del delito en sus diversas formas– temporal –días y horas en que ocurren los delitos– personal –estudio de la víctima y del delincuente– de modus operandi –técnicas y medios materiales empleadas por los delincuentes– y ambiental –estudio de los lugares donde se cometen los delitos– buscando determinar, con ayuda de software informático especial, y la imprescindible habilidad del analista, pautas de acción criminal, prestando atención a reiteraciones que denuncien la actuación de bandas u organizaciones criminales y de delincuentes seriales, tendencias manifestadas por el delito, en definitiva características y

5 Tales como el "Reporte Unificado sobre el delito", sistema unificado de informe de delitos emitido por las policías locales para el Federal Bureau of Investigation (Oficina Federal de Investigación) destinado a posibilitar la elaboración de estadística criminal por parte de dicha oficina, o el más perfeccionado y detallado, derivado del mismo programa, Sistema Nacional de Informes basados en Incidentes vigente en Estados Unidos de América, que contiene, por cada delito informado a la policía o del que ésta toma conocimiento, datos sobre la víctima, el delincuente (cuando es conocido), tipos y valores de los bienes robados, en su caso, características de las personas arrestadas en conexión con el incidente, etc. Un buen sistema de este tipo, adecuadas capacidades de análisis, y constante intercambio de información por vinculación telemática en tiempo real, constituyen herramientas esenciales contra el delito.

reiteraciones del fenómeno delictivo, útiles tanto para prevenir el delito como para investigación de bandas o delincuentes seriales.

El análisis del delito puede contribuir tanto a la inteligencia criminal, como a la investigación criminal.

Mientras en el Reino Unido, otros países anglosajones, y países europeos en general el análisis del delito está plenamente integrado, tanto en los aspectos orgánicos como doctrinarios a la inteligencia criminal –especialmente en sus aspectos tácticos– en Estados Unidos predomina una consideración diferenciada de ambos aspectos[6].

En Estados Unidos, tradicionalmente se ha denominado inteligencia policial (law enforcement intelligence) a la actividad desplegada por agencias federales, tales como el Federal Bureau of Investigation o la Drug Enforcement Administration, enderezada a la identificación y eventual procesamiento de sospechosos de delitos, contribuyendo así a la investigación criminal[7], así como, en las policías locales, a la actividad de inteligencia desarrollada por personal con estado policial (sworn police officers) mientras que el análisis del delito, con las características antes reseñadas, es realizado fundamentalmente por instituciones policiales locales, que cuentan en su seno con analistas sin estado policial, que son sus protagonistas.

En Estados Unidos se suele sintetizar la relación entre ambos, sosteniéndose que mientras el análisis del delito permite saber qué está sucediendo, la inteligencia criminal propiamente dicha permite conocer por qué está sucediendo.

2.4 Denominaciones que recibe la inteligencia criminal en Latinoamérica

La denominación inteligencia criminal aplicada fundamentalmente a la inteligencia sobre el delito, está vigente en el mundo anglosajón –con las peculiaridades ya vistas en Estados Unidos– y en otros países, incluyendo Argentina, no así en la mayoría de los países latinoamericanos.

En Brasil se habla de inteligencia de seguridad pública, concepto de mayor amplitud que el de inteligencia criminal y cercano en sus alcances al anglosajón “security intelligence” –inteligencia de seguridad– aunque también se emplea con frecuencia el concepto de inteligencia policial, referido a la inteligencia sobre el delito en un nivel táctico.

En los restantes países latinoamericanos se habla de “inteligencia policial”, concepto que no solo incluye la inteligencia relativa al delito, sino también cuestiones de orden público y, frecuentemente, de inteligencia política. En definitiva, en dichos países inteligencia policial equivale a actividad de inteligencia llevada a cabo por la policía, debiéndose señalar que en diversos países latinoamericanos la función policial posee significativa amplitud.

3. La organización y características de la inteligencia criminal en aquellos países en los que alcanzó mayor desarrollo

6 OSBORNE, Deborah. “Out of Bonds: Innovation and Change in Law Enforcement Analysis”, Joint Military Intelligence College, Washington D.C., March 2006, p. 18.

7 Ibid.

Habremos a continuación de analizar, con la brevedad impuesta por las características del trabajo, la organización adoptada por la inteligencia criminal en aquellos países en los cuales alcanzó mayor desarrollo: el Reino Unido, Australia, Canadá y, con grandes peculiaridades, Estados Unidos de América.

Los dos modelos más característicos y diversos son los del Reino Unido, seguido, con peculiaridades y limitaciones, por Australia y en menor grado Canadá. Estados Unidos nos presenta un modelo muy diverso, signado por las peculiaridades de su organización policial.

Los cuatro casos tienen, no obstante, aspectos comunes: la actividad de inteligencia criminal es llevada a cabo fundamentalmente por policías, frecuentemente asistidos o complementados por analistas sin estado policial; la actividad está dirigida a conocer en profundidad al delito, a las circunstancias que lo facilitan y lo dificultan y a sus protagonistas, y se realiza conforme a una doctrina –normas y procedimientos– comunes, hallándose vinculados los participantes por una red telemática,

3.1 La inteligencia criminal en el Reino Unido

3.1.1 Orígenes

El origen de la inteligencia criminal está emparentado con la sanción en Inglaterra, en 1829, de la "Metropolitan Police Act" y la correlativa creación de la Policía Metropolitana, citándose la circunstancia de haber sido uno de sus primeros Comisionados Sir Charles Rowan, oficial militar experto en inteligencia.

En 1842 fue creada en la "Metropolitan Police" la "Detective Branch", dedicada a la investigación del delito, sucedida por el "Criminal Investigation Deparment (CID)", que además de desarrollar sus capacidades investigativas, comenzó a producir inteligencia criminal para prevenir el delito y apoyar la investigación criminal, creándose al efecto "C5", una sección de inteligencia. Posteriormente se creó la "Special Branch "(Rama Especial), destinada a prestar apoyo operativo al contraespionaje, a realizar contraterrorismo, a proteger el orden constitucional investigando acciones destinados a alterarlo ilegalmente y a elaborar inteligencia criminal.

Cabe destacar la labor de la Asociación de Jefes de Policía de Inglaterra y Gales (ACPO) proponiendo el desarrollo en las policías de capacidades de inteligencia criminal, así el denominado "Baumber Report" (1975*)* proponiendo la creación de una oficina de inteligencia en cada institución policial, tendiendo especialmente a enfrentar la criminalidad cuyo accionar era interjurisdiccional..

En 1985 fue creada la "NDIU (National Drugs Intelligence Unit*)"* para obtener información y elaborar inteligencia relativa a drogas y narcotráfico.

3.1.2 El NCIS

En abril de 1992, el Ministro del Interior estableció el primer organismo de inteligencia criminal, con competencia general: el Servicio Nacional de Inteligencia Criminal (National Criminal Intelligence Service - NCIS), bajo dependencia del Ministerio del Interior.

Se trató de un organismo dedicado al análisis de información policial y de la que obtenía por sus propios medios, relativa al delito, formulando requerimientos a instituciones

policiales locales y a otros organismos policiales para producir inteligencia criminal y distribuirla entre las referidas instituciones policiales.

La Police Act 1997 (Ley de la Policía de 1997) brindó a este organismo una base legal, habiendo la Police and Criminal Justice Act 2001 (Ley de la Policía y la Justicia Criminal de 2001) y posteriormente la Police Reform Act 2002 (Ley de Reforma Policial de 2002) modificado diversos aspectos no esenciales

Conforme a la ya referida Police Act 1997, constituyeron funciones del NCIS obtener, guardar y analizar información a fin de proveer inteligencia criminal a las fuerzas de policía en Gran Bretaña, a la Real Policía del Ulster, al Escuadrón Nacional contra el Delito, y a otras agencias policiales, y actuar en apoyo de tales fuerzas de policía, y de otras agencias policiales que estén llevando a cabo actividades de inteligencia criminal (Sección 2º).

La ley en cuestión no incluyó al NCIS en la Intelligence Services Act 1994, (Ley de los Servicios de Inteligencia de 1994) norma fundamental que rige la actividad de inteligencia en el Reino Unido, y su régimen legal difiere del conferido en ella.

Existió, sí, coordinación y cooperación entre el NCIS y el Servicio de Seguridad, organismo de inteligencia de seguridad británico.

En lo relativo a la composición del NCIS, la ley estableció (sección 9) que este estaría constituido por policías y otras personas sin estado policial (analistas y personal técnico y administrativo).

Poseía interconexión telemática con las policías locales y otras instituciones con funciones policiales del Reino Unido. Dependía del Ministerio del Interior.

Por otra parte, también, conforme a las órdenes del Ministro del Interior, el NCIS estaba sujeto a las inspecciones llevadas a cabo por los Inspectors of the Constabulary (Inspectores de la Policía), funcionarios a quienes la Police Act 1996 encomienda la inspección de las instituciones policiales británicas para información del Ministro del Interior, verificando la eficiencia y eficacia.

3.1.3 El Modelo Nacional de Inteligencia

Uno de los logros más importantes del NCIS –obtenido en una labor conjunta con la *ACPO*– estuvo constituida por el National Intelligence Model – NIM (Modelo Nacional de Inteligencia), en 1999, instrumento que constituyó un verdadero cuerpo de doctrina –normas, procedimientos y buenas prácticas– destinado a obtener un accionar policial guiado por la inteligencia, por parte del propio NCIS, las policías de Inglaterra y Gales y los organismos británicos participantes en la función policial.

Constituyeron características del NIM las de facilitar la integración de las tareas de obtención de información y elaboración de inteligencia criminal por todos los participantes –el NCIS, el NCS (National Crime Squad*,* organismo de investigación criminal especializada en delito organizado), las policías locales, otros órganos británicos actuantes en seguridad pública– conformándose en tales policías e instituciones, órganos de inteligencia criminal vinculados telemáticamente entre sí en tiempo real, con los correspondientes controles, en tres niveles: local, regional y nacional.

En cada uno de tales niveles se producen documentos de inteligencia estandarizados previstos en el modelo: una evaluación estratégica, que en el nivel nacional constituye la Evaluación de la Situación en el Reino Unido con relación al delito grave y organizado, de nivel estratégico; una evaluación táctica –evaluación del impacto de las operaciones de seguridad, tendencias emergentes en delito o desorden, problemas emergentes– perfiles de problemas, tales como "áreas calientes" de delito o desorden, o delitos seriales y perfiles de blancos o personas de interés para la seguridad pública, tales como delincuentes habituales o profesionales, o redes delictivas determinadas.

La evaluación estratégica, que es producida en los tres niveles ya señalados, constituye un análisis de alto nivel y largo término, de la situación en materia de seguridad pública, conteniendo no solo la situación actual, sino prospectiva de la futura evolución de tal situación.

Los documentos producidos en cada nivel se integran en los producidos en niveles superiores. Por otra parte, la evaluación estratégica de máximo nivel es la base de la que deberán partir los documentos que se produzcan en los distintos niveles.

En todos los niveles se requiere de una respuesta guiada por la inteligencia.

Otro aspecto de interés del NIM es el relativo a las técnicas de análisis empleadas en él.

El NIM comprende también técnicas de análisis específicas destinadas a ser empleadas en inteligencia criminal; análisis de las tendencias en delitos, análisis acerca de cómo funcionan las operaciones o negocios criminales, análisis de las tendencias sociales y poblacionales, análisis de mercado criminal, análisis de redes criminales, análisis de blancos, evaluación operacional de inteligencia criminal, análisis de resultados, análisis de riesgos, etc.

3.1.4 La SOCA

En otro orden de ideas, cabe destacar que la Serious Organised Crime and Police Act 2005 determinó la fusión del NCIS, del NCS, y del Customs National Investigation Service en un nuevo organismo de inteligencia criminal con funciones ejecutivas de investigación criminal, la Serious Organised Crime Agency (SOCA), que comenzó su funcionamiento el 3 de mayo de 2006, cuya actividad estuvo centrada fundamentalmente en la lucha contra el delito grave y organizado nacional y trasnacional, aunque manteniendo el apoyo de inteligencia criminal que brindaba el NCIS a las policías locales británicas.

Conforme al artículo 2°, eran funciones de la SOCA …prevenir y detectar delito grave y organizado, y contribuir a la reducción de ese delito de otras maneras, y a mitigar sus consecuencias…

Por otra parte, el artículo 3 le asignó la función de "…obtener, guardar, analizar y diseminar información relevante para la prevención, detección, investigación y prosecución de delitos, y para la reducción del delito de otras maneras, y la mitigación de sus consecuencias…"

Como puede advertirse, se había optado por unificar en un mismo organismo las funciones de investigación del delito organizado y obtención de información y de elaboración de inteligencia criminal, sin confundirlas.

La conducción de la SOCA estaba a cargo de un órgano colegiado, a cuya cabeza estaba un presidente designado por el Secretario del Interior, y que comprendía miembros ex officio –el Director General de la SOCA, que constituía la autoridad ejecutiva del organismo– y miembros del organismo propuestos por él y los miembros ordinarios, en número igual a los indicados precedentemente, designados por el Secretario de Estado.

Su conducción ejecutiva era ejercida por el Director General, designado por el Secretario del Interior por un término que no podía exceder cinco años,

Entre las facultades del Director General estaba la de asignar a miembros de su personal las plenas facultades de un policía, de un agente de aduanas, o de un funcionario de inmigración.

La SOCA continuó prestando apoyo de inteligencia a las policías locales y a otros organismos con funciones policiales, así como aplicando el Modelo Nacional de Inteligencia y elaborando la Evaluación del Reino Unido sobre la Amenaza Representada por el Delito Grave y Organizado.

3.1.5 La NCA

La Ley del Delito y de los Tribunales de 2013 dio lugar a la creación de un nuevo organismo de inteligencia criminal con importantes funciones ejecutivas de investigación criminal y lucha contra el delito, surgido de la fusion de la *SOCA c*on otras instituciones y organismos de seguridad pública británicos, la Agencia Nacional contra el Delito (National Crime Agency – NCA).

La Agencia Nacional del Delito es un organismo de inteligencia criminal que posee también facultades para realizar investigación criminal especializada fundamentalmente sobre delito grave y organizado, así como para impartir órdenes a otras instituciones policiales inglesas para luchar contra el delito.

Actúa tanto produciendo inteligencia criminal, con información que obtiene por sus propios medios y de otras policías británicas y de otros organismos británicos, como llevando a cabo investigación criminal especializada, proveyendo además a otras policías apoyo especializado de inteligencia criminal y de investigación criminal, y brindando liderazgo nacional para obtener que las policías británicas optimicen el uso de sus recursos y los empleen más eficazmente.

La NCA procura construir un único y comprensivo panorama del delito grave y organizado, obteniendo información de una variedad de fuentes y elaborando inteligencia, que dirige su propia actividad operacional y la de sus socios: las policías británicas y otros organismos británicos con funciones policiales.

Cabe destacar que la Unidad de Inteligencia Financiera del Reino Unido (United Kingdom Financial Intelligence Unit – UKFIU) funciona dentro de la NCA y con el apoyo de ésta, constituyendo el instrumento fundamental para la lucha contra el lavado de activos.

Según su ley de creación, la NCA cumple las siguientes funciones, entre otras:

a) La función de reducción del delito, consistente en asegurar la realización de actividades eficientes y efectivas para combatir el delito organizado y el delito grave, ya sea por la propia NCA, otras instituciones policiales, u otras personas;

b) La función de inteligencia criminal, consistente en obtener, guardar, procesar, analizar y diseminar información que sea relevante para actividades para combatir delito organizado o delitos graves, actividades para combatir cualquier otra clase de delitos, investigaciones sobre explotación de productos de delitos;

c) Cumple funciones también en materia de protección de menores, y de proveer asistencia para la lucha contra el delito organizado a países extranjeros.

3.1.6 Conclusiones

En suma, actualmente el Reino Unido se caracteriza por poseer un organismo de inteligencia criminal con muy importantes funciones ejecutivas de investigación criminal y de lucha contra el delito. Como organismo de inteligencia criminal, apoya la tarea en la materia de las policías locales y de otros organismos con funciones policiales, actuando interconectados telemáticamente y conforme a una doctrina común.

Su personal tiene actualmente una composición más variada. Si bien el NCIS formado originariamente por personal policial especializado adscripto, personal policial retirado incorporado permanentemente, y analistas sin estado policial, además de personal administrativo, hoy incorpora personal originariamente perteneciente a otros sectores de la administración pública e incluso del sector privado. Si bien hasta fecha reciente todos sus Directores Generales habían sido policías, su actual Director General, Graeme Biggar, es un funcionario público con destacada carrera en diversas áreas, fundamentalmente de seguridad nacional.

El Modelo Nacional de Inteligencia continúa constituyendo el marco fundamental del accionar policial británico. La legislación que rige la inteligencia criminal continúa siendo diversa a la que rige la actividad de inteligencia, como también son diversos los controles que ambas actividades poseen, más allá de los puntos comunes en materia de control que surgen de la Ley de Regulación de Poderes Investigativos del 2000 (Regulation of Investigatory Powers Act 2000) y su modificatoria del 2016.

3.2 Estados Unidos de América

3.2.1 Orígenes de la inteligencia criminal en Estados Unidos

La inteligencia criminal también tiene raíces antiguas en la actividad policial estadounidense, al igual que en el Reino Unido, aunque sustanciales diferencias con este *último país*, relacionadas con las peculiaridades de la actividad policial estadounidense, probablemente la m*ás* descentralizada del mundo.

Estados Unidos tiene alrededor de 18.000 instituciones policiales, que comprenden policías municipales, de condado, tribales, policías especiales, estaduales y nacionales.

La tradición anglosajona de gobierno local autónomo ha determinado que las ciudades y pueblos tengan discrecionalidad en la organización de sus policías; si bien los estados

locales tienen facultades para establecer estándares mínimos para las policías locales existentes dentro del estado.

Además de las policías locales, Estados Unidos cuenta con importantes instituciones nacionales con funciones en seguridad pública, como la Oficina Federal de Investigación, organismo federal de investigación que es al mismo tiempo un organismo de inteligencia y de contrainteligencia, brindando asimismo apoyo técnico a policías locales; el Departamento de Seguridad Interna (Department of Homeland Security) ministerio que agrupa a múltiples agencias civiles con funciones policiales y de protección civil, incluyendo una policía naval con estructura militar, United States Coast Guard (Guardacostas de Estados Unidos) y un organismo de investigación y protección de personalidades, el Servicio Secreto de Estados Unidos. También cuenta Estados Unidos con un organismo de investigación e inteligencia con funciones en narcotráfico y drogas, la Drug Enforcement Administration (DEA), así como con la Oficina de Alcohol, Tabaco, Armas de Fuego y Explosivos (ATF) organismo de investigación *y control sobre dichos temas, entre otros.*

En Estados Unidos de América existe cierta distinción entre la inteligencia criminal producida por dichos organismos nacionales, y la inteligencia criminal producida por las policías locales.

Estados Unidos de América no cuenta con legislación ni con un organismo específico de inteligencia criminal, surgiendo cierta coordinación de ésta como consecuencia de los atentados del 11 de Septiembre de 2001 y la necesidad de sumar a las policías locales a la vigilancia y prevención contra el terrorismo de raíz musulmana.

El surgimiento de la inteligencia criminal tuvo lugar a partir de la década de los 20[8] cuando las policías, el Departamento del Tesoro y la FBI comenzaron a obtener información sobre anarquistas o gánsteres, y en la década de los 60 con relación a las grandes organizaciones criminales.

A partir de las décadas de los 40 y 50 creció el uso de la inteligencia criminal contra tales organizaciones, fundamentalmente contra la Mafia –La Cosa Nostra y sus derivaciones, que con la prohibición habían obtenido grandes ganancias y que tras su finalización en 1933 mutaron a otras formas delictivas– fundamentalmente, fraudes, extorsión, etc., infiltrándose además en negocios lícitos[9].

En Estados Unidos, la inteligencia criminal fue desarrollada tanto en instituciones nacionales como la FBI, la AFT y la DEA, como en diversas policías locales, especialmente en aquellas de mayor tamaño y recursos, con diferencias organizacionales y conceptuales, e inicialmente muy limitadas vinculación y cooperación.

En 1956 fue creada la Association Law Enforcement Intelligence Units (LEIU-Asociación de Unidades de Inteligencia Policial), formada inicialmente por 26 agencias estaduales y locales, para intercambiar información confidencial sobre delito organizado, totalizando su membresía actualmente 240 agencias policiales en tres países, comprendiendo sus ac-

8 PETERSON, Marilyn B. *Application in Criminal Analysis: A Sourcebook,* Praeger, Westport, 1994, pp. 2-3.

9 HARRIS. Loc. Cit.

tividades la formación de personal, la comunicación y el intercambio legal y ético de información, en materia de inteligencia criminal[10].

En 1980 se creó la Asociación Internacional de Analistas de Inteligencia Criminal (IALEIA), organización en creciente expansión en diversos países, cuyo propósito estuvo dirigido a la profesionalización del análisis de inteligencia policial, brindando talleres de entrenamiento y capacitación en análisis y aspectos vinculados a la inteligencia criminal y al delito organizado.

En 1970, y sobre la base del trabajo de la Comisión Presidencial sobre Delito Organizado, tuvo lugar la sanción de la Racketeer[11] and Corrupt Organizations Act (RICO) (Ley sobre Organizaciones Criminales y Corruptas). Esta ley estableció la ilegalidad de adquirir, operar, o recibir ingresos de una empresa, a través de una pauta de delito organizado, castigando además la pertenencia, conducción, o participación en los negocios de empresas cuya actividad incluyera comercio interestatal y comprendiera la realización, participación o cooperación en los delitos descriptos en la norma.

La creación de los Sistemas Regionales para Compartir Información (RISS) sistema de interconexión para intercambio de información y apoyo técnico, organizado y financiado por el Gobierno Federal y administrado regionalmente, incluyó el suministro de herramientas analíticas para un número significativo de agencias y, consiguientemente, de personal, comenzando su funcionamiento en 1971, llegando a nuclear más de 9.400 agencias policiales y de seguridad pública federales, estaduales, locales y tribales, incluyendo usuarios en todos los estados locales y el Distrito de Columbia, así como en territorios estadounidenses, y en Inglaterra, Nueva Zelandia y partes de Canadá[12].

En 1981 tuvo lugar la creación de la Asociación Internacional de Analistas Criminales (IACA), organización destinada a asistir a agencias que establecieran unidades de análisis criminal y para brindar adiestramiento y capacitación en inteligencia criminal, poseyendo actualmente más de 2.000 miembros en 50 países.

Asimismo, la Asociación Internacional de Jefes de Policía (IACP), además de participar a IALEIA en varias de sus actividades, desarrolló un manual de administración en la materia, Criminal Intelligence (IACP, 1985).

También en 1985 comenzó el funcionamiento, en la FBI, de Law Enforcement On Line (LEO).

Se trata de un acceso controlado para comunicaciones y repositorio de datos e información compartida para la labor policial para personal policial, primeros respondedores,

---

10 MOREHOUSE Bob. Op. Cit. p. 4.

11 La expresión “racketeering activities” hace referencia a múltiples actividades delictivas, fundamentalmente practicadas por organizaciones criminales, detalladas en la definición contenida en 18 U.S. Code § 1961.

12 U.S. DEPARTMENT OF JUSTICE, Office of Justice Programs. (En línea) Regional Information Sharing Systems Program. (Fecha de consulta 14 de mayo de 2024). Disponible en : https://www.ojp.gov/pdffiles1/bja/192666.pdf. U.S. HOUSE OF REPRESENTATIVES. (En Línea) Regional Information Sharing Systems Program (Fecha de consulta 14 de mayo de 2024). Disponible en: https://docs.house.gov/meetings/AP/AP19/20130321/100498/HHRG-113-AP19-Wstate-KennedyD-20130321.pdf

profesionales de la justicia criminal, y agencias antiterroristas y de inteligencia de Estados Unidos y con participación de diversos países, certificado, controlado y dirigido por la FBI.

También NLETS, National Law Enforcement Telecomunication System (Sisterma Nacional de Telecomunicación Policial) es una red creada entre las policías estaduales y manejada por estas –sin intervención directa de los estados a los que sirven, ni del Gobierno Federal– a través de la cual se intercambian datos de carácter policial y criminal.

Asimismo, la DEA mantiene una diversidad de programas que involucran la cooperación y trabajo conjunto con policías estaduales y locales estadounidenses, entre los que se destacan las HIDTAs (High Intensity Drug Trafficking Areas, que procuran apoyar la cooperación entre los órganos policiales federales, estaduales y locales, y de salud federales, para luchar contra el narcotráfico y limitar los efectos en la salud pública de las drogas ilícitas.

En definitiva, en Estados Unidos se ha producido una creciente divulgación y desarrollo de técnicas de análisis, y creación de redes de o con incidencia en inteligencia criminal.

La característica descentralización del sistema estadounidense, se traducía en un accionar policial y de inteligencia criminal centrado fundamentalmente en los aspectos locales, sin perjuicio de la actuación de las ya referidas agencias investigativas federales, en delitos de carácter federal y de seguridad nacional.

3.2.2 Los atentados del 11 de Septiembre de 2001

Los atentados del 11 de Septiembre de 2001 produjeron cambios fundamentales en la situación descripta.

Así, se creó un Ministerio (Departamento Ejecutivo) de Seguridad Interna –Department of Homeland Security DHS– con sustantivos poderes, al que fueron incorporados diversos organismos vinculados con la seguridad interna, y se estableció una coordinación nacional en materia de inteligencia criminal, que anteriormente había estado fundamentalmente ausente.

La Ley de Seguridad Interna del 2002 brindó marco legal a la creación del referido Departamento Ejecutivo, determinando su misión y funciones, fundamentalmente prevenir ataques terroristas en el territorio estadounidense y disminuir su vulnerabilidad a tales ataques, minimizar los daños y su recuperación, estableciéndoselo como punto focal en materia de desastres naturales y provocados por el hombre, encomendándosele además el monitoreo de eventuales conexiones entre el tráfico de drogas ilegales y el terrorismo, entre otros aspectos.

Se estableció dentro del DHS el Directorio para Análisis de la Información y Protección de Infraestructura, previsto en la Sección 201 de la ley, dirigido por un Subsecretario de Análisis de Información y Protección de Infraestructura, a quien se asignó, entre otras funciones, las de acceder, recibir y analizar información e inteligencia policial, así como información de agencias de los gobiernos federal, estaduales y locales y entidades del sector privado; así como integrar tal información para identificar y evaluar la naturaleza y ámbito de las amenazas terroristas para el país, y detectar e identificar amenazas de terrorismo contra Estados Unidos.

Fue dispuesto además que el DHS contaría con un staff de experimentados analistas.

Cabe destacar los esfuerzos producidos, a partir de la creación del DHS, con el apoyo del Departamento de Justicia, por parte de la Asociación Internacional de Jefes de Policía, para establecer adecuados mecanismos para compartir información e inteligencia entre órganos policiales nacionales, estaduales, locales y tribales, y organismos de inteligencia, a partir de la Cumbre para Compartir Inteligencia Criminal[13].

Esa tarea se reflejó, tras varias etapas, en la formulación del Plan Nacional para compartir Inteligencia Criminal[14], producido bajo la guía y dirección del Departamento de Justicia, que previó estándares mínimos en materia de obtención, entrega, almacenamiento y diseminación de inteligencia criminal, la definición de la administración y supervisión de dicha función, estándares para adiestramiento del personal en inteligencia criminal, el desarrollo por las instituciones policiales de capacidades de registro y procesamiento automático de datos, constituyendo bases de datos centradas en incidentes, tanto para uso propio como para interconexión telemática con sistemas de información estaduales y federales.

Fue contemplada la interconexión del Sistema Regional para Compartir Información (RISS) y el Sistema del FBI de Actividad Policial en Línea (LEO), requiriéndose la interoperabilidad de todos los sistemas informáticos de las instituciones policiales del país de todos los niveles, con el sistema RISS/LEO.

Cabe destacar, en materia de estándares normativos, la adopción de los establecidos por vía reglamentaria en 28 CFR 23, así como por la Directiva sobre Archivos de Inteligencia Criminal de LEIU[15], aspectos estos que desarrollaremos más adelante

El Plan, *más que constituir un cuerpo doctrinario como* el NIM inglés, se limitó a asegurar la interconexión telemática entre los participantes y a establecer mecanismos adecuados para compartir información, preservando los derechos individuales, procurándose además asegurar la existencia de un lenguaje y conceptos comunes, así como estándares mínimos de entrenamiento y conocimiento.

Cabe destacar que el Plan contuvo definiciones destinadas evidentemente a disminuir las disimilitudes conceptuales existentes en el complejo universo policial estadounidense y a avanzar hacia un lenguaje común.

---

13 U.S. DEPARTMENT OF JUSTICE, GLOBAL JUSTICE INFORMATION SHARING INITIATIVE. (2003) The National Criminal Intelligence Sharing Plan, p. 14. (En línea) (Fecha de Consulta 1 de mayo de 2024). Disponible en: https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/national_criminal_intelligence_sharing_plan.pdf

14 Global Justice Information Sharing Initiative, United States Department of Justice, National Criminal Intelligence Sharing Plan, Washington, 2003.

15 Association of Law Enforcement Intelligence Units (Asociación de Unidades de Inteligencia Policial), una asociación cuya misión es la de "…proveer liderazgo y promover profesionalismo en la comunidad de inteligencia criminal para proteger la seguridad pública y los derechos constitucionales..." Se trata, en definitiva, de una organización de cooperación entre instituciones policiales estadounidenses para el establecimiento de estándares, buenas prácticas e intercambio de información entre más de 240 instituciones policiales federales, estaduales y locales en Estados Unidos.

En Estados Unidos no existe un organismo de inteligencia criminal cabeza de la estructura de inteligencia criminal, como existe en el Reino Unido y como veremos en Australia y Canadá, entre otros países,

Un aspecto de interés e importancia en el análisis de las estructuras de inteligencia criminal en Estados Unidos de América, es el relativo a las estructuras de cooperación en inteligencia entre el Estado Nacional y los gobiernos estaduales, locales y tribales, creadas fundamentalmente para enfrentar la amenaza terrorista.

Con tal propósito se establecieron, por una parte, la Fuerza Nacional Conjunta de Tareas contra el Terrorismo y las Fuerzas Conjuntas de Tareas contra el Terrorismo –NJTTF y JTTF– encabezadas por la FBI sumando a instituciones policiales estaduales, locales y tribales, por una parte, y por la otra los Centros de Fusión (Fusion Centers), órganos de inteligencia antiterrorista y criminal organizados por los estados locales, con apoyo de financiamiento, tecnológico y de personal por parte del Departamento de Seguridad Interna –DHS– Department of Homeland Security. Analizaremos a continuación ambas iniciativas.

Cabe recordar que la FBI era, con anterioridad a la creación del *DHS*, la responsable primaria de la inteligencia antiterrorista en territorio estadounidense,

Después de la creación del DHS, la FBI continuó desarrollando una actividad de inteligencia antiterrorista.

Así, la NJTTF constituye un órgano que produce inteligencia antiterrorista formulando requerimientos a diversos órganos de la FBI, y de coordinación, y de apoyo administrativo, logístico y de adiestramiento a las JTTF, que constituyen unidades operacionales dirigidas por la FBI e integradas por personal de dicho organismo y de otras instituciones de seguridad nacionales y locales, que realizan investigaciones de campo y producen inteligencia relativas a amenazas terroristas actuales y potenciales, con un amplio despliegue en el territorio estadounidense.

Las JTTF existían con anterioridad al 11 de septiembre de 2001[16] no así la NJTTF, cuya creación tuvo origen en la percepción incrementada de la amenaza terrorista tras estos atentados y el consiguiente aumento del número y despliegue de las JTTF, la necesidad de su coordinación, y de un centro de apoyo y de análisis de inteligencia, constituido por la NJTTF, para la información e inteligencia originada en las JTTF.[17]

En definitiva, se trata de órganos de investigación criminal y de elaboración de inteligencia, dirigidos fundamentalmente contra terrorismo internacional y doméstico y actividad criminal vinculada al terrorismo, que procuran evitar actos terroristas, dirigidas por la FBI, y que incluyen tanto miembros propios, habitualmente en mayor proporción, y de otras agencias e instituciones federales, estaduales y locales, y que funcionan en las Oficinas de Campo y en algunas Oficinas Residentes de dicho organismo.

16 U.S. DEPARTMENT OF JUSTICE, OFFICE OF THE INSPECTOR GENERAL, June 2005 (En Lìnea) The Department of Justice's Terrorism Task Forces Evaluation and Inspections Report I-2005-007. (Fecha de Consulta 1 de mayo de 2024). Disponible en https://oig.justice.gov/reports/plus/e0507/index.htm

17 Ibid. p. 21.

Por otra parte, encontramos organizados por la DHS los Centros de Fusión, que también surgieron tras los atentados como una respuesta al desafío representado por el terrorismo y la necesidad de alistar en la protección de la seguridad del país a la totalidad de las aproximadamente 18.000 agencias con funciones policiales y cerca de un millón de empleados, incluyendo policías (sworn officers), analistas y otros colaboradores[18], particularmente en la detección de actividades terroristas y sospechosas de serlo, incluyéndose también otras actividades delictivas, particularmente de delito organizado, por haberse detectado casos de actividades de ese tipo llevadas a cabo por células terroristas.

Dicho alistamiento para cooperación en la seguridad nacional y especialmente en el contraterrorismo, incluyó a instituciones de protección civil, así como de salud y de transporte, y al sector privado, cuyas empresas son propietarias de la mayor parte de la infraestructura crítica del país.

El desafío supuso la necesidad de que la Comunidad de Inteligencia de Seguridad Nacional estadounidense compartiera información e inteligencia antiterrorista a los restantes participantes, y que estos compartieran la información de que dispusieran relativa a posibles actividades terroristas u otras significativas actividades criminales, y que ello ocurriera respetando la privacidad y demás derechos civiles de los ciudadanos y residentes legales estadounidenses.

Los Centros de Fusión son establecidos y mantenidos conforme a las Fusion Center Guidelines (Directivas sobre Centros de Fusión) elaboradas por el Departamento de Justicia, en colaboración con el Departamento de Seguridad Interna de Estados Unidos[19]. La decisión para establecerlos es estadual, siguiendo las directivas nacionales, así como su dirección es estadual o local según el caso, sujeto en última instancia a la autoridad estadual, pero el Estado Nacional colabora con su financiación y equipamiento, así como con el suministro de personal especializado.

La característica fundamental de tales Centros de Fusión es la de recibir información de toda fuente, desde organismos de inteligencia de seguridad nacional, hasta empresas privadas, pasando por el muy numeroso y variado universo policial estadounidense, y, al propio tiempo, posibilitar que la información e inteligencia antiterrorista elaborada por los organismos de seguridad nacional llegue en la medida necesaria a consumidores –y suministradores– *no tradicionales,* que deben recibirla para orientarse para suministrar información y adoptar las precauciones que fueren necesarias.

Cabe destacar la existencia de la Red Nacional de Centros de Fusión –National Network of Fusion Centers[20]–, a través de la cual se canaliza el ya señalado flujo de informa-

18 La FBI determinó 1.003.270 empleados (2019) de agencias policiales, incluyendo tanto policías, como colaboradores y personal auxiliar. V. https://ucr.fbi.gov/crime-in-the-u.s/2019/crime-in-the-u.s.-2019/topic-pages/tables/table-74

19 U.S. DEPARTMENT OF JUSTICE, BUREAU OF JUSTICE ASSISTANCE, GLOBAL JUSTICE INFORMATION SHARING INITIATIVE, august 2006 (En Línea) Fusion Center Guidelines, Executive Summary. (Fecha de consulta 1 de mayo de 2024). Disponible en: https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/fusion_center_executive_summary.pdf

20 INTELLIGENCE AND ANALYSIS. Fusion Centers. (En Lìnea). (Fecha de Consulta 1 de mayo de 2024). Disponible en: https://www.dhs.gov/fusion-centers

ción e inteligencia de dos vías entre el Gobierno Federal, los Gobiernos estatales, locales, tribales y territoriales, y organizaciones del sector privado.

Un Centro de Fusión debe poseer capacidades para: Planificar y Desarrollar Requerimientos (de información e inteligencia), obtener y reunir información (en el caso de la obtención, a través de las instituciones y entidades que brindan información), reconocer indicadores y alertas, procesar y cotejar información, realizar análisis de inteligencia y realizar productos de inteligencia, diseminar información e inteligencia, y efectuar reevaluación. Debe, además, proteger la privacidad de los ciudadanos y de la información, brindar seguridad a la información, adecuado personal, entrenamiento, poseer adecuada tecnología e infraestructura, así como sistemas, equipamiento, instalaciones, de la información y de las comunicaciones, e infraestructura física, así como financiamiento.

Se requiere que los Centros de Fusión realicen o contribuyan a la realización, según el caso, de una Evaluación de Riesgo estadual y/o regional, que identifique y priorice amenazas, vulnerabilidades y consecuencias a intervalos regulares.

Frente a la complejidad y variedad de esfuerzos existentes en Estados Unidos en materia de inteligencia criminal, no han faltado voces de alerta respecto a la variedad y complejidad del sistema y a las siempre posibles superposiciones.

Resulta elocuente al respecto un informe de la Oficina de Contabilidad General (General Accounting Office) órgano de control externo de la Administración Pública estadounidense, dependiente del Congreso[21]:

Dicho informe destaca que "…Cinco tipos de entidades de intercambio de información de campo son apoyadas, en parte, por el gobierno federal –Fuerzas de Tareas Conjuntas sobre terrorismo, Grupos de Inteligencia de Campo, Sistemas Regionales de Intercambio de Información (RISS), centros de fusión estaduales y de mayores áreas urbanas, y Centros de Apoyo Investigativo de Áreas de Alta Intensidad de Narcotráfico (HIDTA)–, que tienen distintas misiones, roles y responsabilidades. Sin embargo, GAO identificó 91 instancias de superposición en ciertas actividades analíticas –tales como la producción de informes de inteligencia– y 32 instancias de superposición en actividades de apoyo investigativo, tales como identificar lazos entre organizaciones criminales. Estas entidades llevan a cabo actividades similares dentro de la misma área de misión, tales como contraterrorismo, para clientes similares, tales como agencias federales o estaduales. …GAO también encontró que los centros RISS y las HIDTA operaban tres sistemas diferentes que duplicaban la misma función, identificar cuándo diferentes entidades policiales podían estar llevando a cabo una similar acción operativa, tal como un raid en el mismo lugar, para asegurar la seguridad de los oficiales…Las agencias no tienen entidades responsables de la coordinación, ni oportunidades evaluadas para mejorar la coordinación, para ayudar a reducir el potencial para superposición y alcanzar eficiencias…"

Lo cierto es que poderosas instituciones dotadas de importantes recursos económicos, sofisticada tecnología y personal adecuadamente formado y adiestrado –fundamental-

21 GENERAL ACCOUNTING OFFICE. INFORMATION Sharing: Agencies Could Better Coordinate to Reduce Overlap in Field-Based Activities. Informe 13-471 de abril 2013. Fecha de consulta 22 de febrero de 2021. Disponible en: https://www.gao.gov/products/gao-13-471

mente DHS, FBI y DEA– pugnan entre sí por presupuesto, logros y por sumar a sus propias esferas, en el mayor número y grado posible, a la constelación de policías estaduales, locales y tribales estadounidenses, que incluyen a instituciones tan grandes como el New York Police Department –NYPD– y a otras que poseen exclusivamente 1 o 2 efectivos.

Examinando las policías estaduales y locales en materia de inteligencia criminal, debemos destacar que existe una gran variedad de estructuras y de organización del personal.

En muchas policías estaduales y locales existen analistas criminales que realizan tareas de *análisis del delito.* En algunas otras, son los policías *(sworn officers)* quienes realizan tales tareas de análisis. Existen diversidades respecto de la tarea que cumplen los analistas, que incluyen la propia denominación de su labor.

Una peculiaridad estadounidense en inteligencia criminal fue el importante rol desempeñado en su desarrollo por los analistas criminales. Esta función fue y es desempeñada en apreciable parte por mujeres, habiendo estado entre sus más destacadas cultoras Marilyn Peterson, Deborah Osborne y Rachel Boba, que de posiciones modestas en instituciones policiales locales, devinieron destacadas autoras, funcionarias y docentes universitarias.

La actividad de los analistas incluyó tanto la investigación criminal como la inteligencia criminal. Por otra parte, careciendo en su gran mayoría de estado policial, los analistas colaboraban con la actividad de los oficiales de policía (sworn officers*) únicos capaces de progresar en su carrera, alcanzar altos rangos e inclusive ocupar jefaturas en instituciones policiales de mayor importancia,*

La actividad realizada por los analistas pasó a llamarse, ya sea análisis criminal, incluyendo la tarea de análisis realizada dentro del ámbito de la justicia criminal, comprendiendo tanto a policías como a fiscalías, e incluso a otros organismos fundamentales, fundamentalmente de conducción de la seguridad pública –y hasta al sector privado– como, más específicamente, análisis del delito (crime analysis), refiriéndose a la determinación de pautas y tendencias criminales a través de la minería de datos.

La denominación de inteligencia criminal fue habitualmente reservada para la obtención y análisis de información realizada por los oficiales de policía o, fundamentalmente, por las agencias investigativas federales, especialmente las ya referidas FBI, DEA y ATF*,* relativa a sospechosos, delincuentes conocidos y a organizaciones criminales, es decir, fundamentalmente a personas.

Un aspecto de interés de la inteligencia criminal estadounidense es el relativo a las bases legales que dicha actividad posee, incluyendo la protección de la privacidad.

Cabe destacar en primer lugar el capítulo 28, parte 23 del Código de Regulaciones Federales (28 CFR 23), sustentado en la Omnibus Crime Control and Safe Streets Act de 1968, Public Law 90-351 as amended (Ley de Control del Delito General y de Calles Seguras, Ley Pública 90-351 y sus enmiendas), que señalando que el delito era ante todo un problema local, facultó al Estado Nacional, Departamento de Justicia, a otorgar subsidios (grants) a los estados locales que formularan amplios planes aprobados por el Estado Nacional para fortalecer y mejorar la seguridad pública en diversos aspectos, entre los cuales la ley inclu-

yó "… el desarrollo de sistemas para recolectar, guardar, y diseminar información relativa al delito organizado…"

En consecuencia, 28CFR23 constituye una reglamentación federal de una ley federal de apoyo a los estados locales para la lucha contra el delito.

Por ello, esta reglamentación se aplica exclusivamente a los sistemas de inteligencia criminal estaduales o locales financiados total o parcialmente a través de la ley antes referida, así como a los sistemas de inteligencia criminal operados por organismos federales. No obstante, ha pasado a constituir un estándar que goza de amplia aplicación y que es reconocido y observado en la generalidad de los casos.

Entre los requisitos establecidos por la norma en análisis para que una agencia pueda ser beneficiaria de la financiación que dispone, se encuentra que posea "…facultades policiales o de investigación criminal y que está autorizada para enviar y recibir información de inteligencia criminal a través de un sistema interjurisdiccional de inteligencia…"

Un aspecto fundamental es el requisito relativo a que "…Un proyecto recolectará y mantendrá información de inteligencia criminal relativa a un individuo sólo si hay razonable sospecha de que el individuo está involucrado en una conducta o actividad criminal y que la información es relevante a esa conducta o actividad criminal…" prohibiéndose recolectar o mantener "información de inteligencia criminal sobre las opiniones, asociaciones o actividades políticas, religiosas o sociales de cualquier grupo, asociación, corporación, negocio, asociación, u otra organización, a menos que tal información sea directamente relativa a actividad o conducta criminal y que haya una sospecha razonable de que el sujeto de la información está o puede estar involucrado en una conducta o actividad criminal…".

Se establece el requisito de Razonable Sospecha o el Predicado Criminal, que concurren "…cuando existe información que establece hechos suficientes para dar a un funcionario policial o investigador criminal de una agencia, investigador, o empleado entrenados, una base para creer que hay una posibilidad razonable de que un individuo u organización está involucrado en una actividad o empresa criminal definibles…"

Se prohíbe incluir información "…que haya sido obtenida en violación de cualquier ley u ordenanza federal, estadual o local…"

Se exige para diseminar información que haya una necesidad de conocer y un derecho a conocer la información en el cumplimiento de una actividad policial…

Se impone además la obligación, cuando se mantenga información de inteligencia criminal, que "…sean adoptadas salvaguardas administrativas, técnicas y físicas (incluyendo procedimientos de auditoría) para asegurar tal información contra acceso no autorizado y contra daño intencional o no intencional..."

Además de los estándares establecidos en el 28 CFR 23, también tienen importancia las "Directivas en Materia de Archivos de Inteligencia Criminal" (Criminal Intelligence File Guidelines) elaboradas por la asociación Unidad de Inteligencia Policial (Law Enforcement Intelligence Unit –LEIU–). Ambas son recomendadas en el Plan Nacional para Compartir Inteligencia Criminal.

Se trata de un cuerpo de normas en definitiva emanadas de una asociación profesional privada de gran prestigio, pero en definitiva sin fuerza obligatoria. Son en definitiva muy semejantes a las ya vistas en 28 CFR 23, conteniendo también el predicado criminal.

En definitiva, preciso es reconocer, como señala John Gordnier, que en Estados Unidos "…las leyes federales que predominan en la arena de la seguridad nacional no se aplican, en su mayor parte, a los esfuerzos estaduales y locales de inteligencia criminal…"[22]

Por otra parte, después del 11 de septiembre de 2001, como se ha visto, las policías estaduales, locales y tribales han pasado a colaborar de forma constante y rutinaria con agencias federales con funciones de seguridad nacional, como el Departamento de Seguridad Interna (DHS), y la Oficina Federal de Investigación (FBI), con las características antes señaladas.

El aspecto fundamental que caracteriza a la inteligencia criminal en Estados Unidos, es el de ser el resultado de legítima actividad policial, por una parte, y el predicado criminal, es decir, la inevitable referencia a una actividad criminal conocida o que constituye objeto de una sospecha razonable.

Más que una base legal específica, la inteligencia criminal en Estados Unidos –fundamentalmente local, como se ha visto– está regida por conceptos fundamentalmente jurisprudenciales y reflejados en los ya señalados cuerpos normativos 28 CRF 23 y las Directivas de LEIU, que gozan de reconocimiento general y recibieron apoyo en el Plan Nacional para Compartir Inteligencia Criminal. En definitiva, su vigencia reside fundamentalmente en su aceptación y en la manera en que reflejan los estándares constitucionales, legales y jurisprudenciales vigentes.

En definitiva, la facultad de la policía estadounidense para obtener, reunir, guardar en un archivo de inteligencia criminal y analizar información relativa a personas –incluyendo personas estadounidenses– se basa en los ya señalados conceptos de propósito policial legítimo y sospecha razonable.

En otro orden de ideas, la inteligencia criminal estadounidense emplea técnicas de análisis que, comparadas con las contenidas en el MIN inglés, permite advertir el carácter más táctico de las vigentes en Estados Unidos, circunstancia derivada de las ya señaladas características del sistema policial estadounidense, técnicas que como sucede también en el Reino Unido, son auxiliadas por conocidos programas informáticos. Remitimos en la materia a la destacada analista criminal Marilyn Peterson, tanto en la que consideramos su obra fundamental[23] como en un trabajo posterior[24], así como en una obra coeditada con otro importante analista estadounidense, Paul P. Andrews[25].

---

22 GORDNIER John. *Legal Issues in U.S. Criminal Intelligence: An Overview,* en MOREHOUSE, Bob, PETERSON, Marylin B. and PALMIERI, Lisa (Eds.). *Criminal Intelligence for the 21st Century,* IALEIA-LEIU, Richmond, 2019, p. 16.

23 PETERSON, Marilyn B. "Applications in Criminal Analysis. A sourcebook".Praeger, Westport, 1998, pp. 29-60.

24 PETERSON, Marilyn B. Analysis and Synthesis, en MOREHOUSE, Bob. "et al". Op. Cit. pp. 88-108.

25 ANDREWS, Paul P., Jr. y PETERSON, Marilyn B. "Criminal Intelligence Analysis", Palmer Enterprises, Loomis, 1990.

En conclusión, podemos señalar como características fundamentales del modelo estadounidense de inteligencia criminal su carácter fundamentalmente táctico, surgido de la cotidiana lucha contra el delito y su base predominantemente local, derivada de la notable descentralización de su sistema policial, sin perjuicio de los esfuerzos de coordinación y apoyo de grandes instituciones federales, fundamentalmente FBI, DEA y ATF, y de la tarea constante del Departamento de Justicia.

La lucha contra el terrorismo ha pasado a constituir un nuevo y poderoso factor, acentuado tras los atentados del 11 de Septiembre de 2001 y la subsiguiente creación del DHS, originándose así los Centros de Fusión que, en conjunción con las JTTF motorizadas por la FBI, han procurado sumar a las policías estaduales, locales y tribales a la lucha contra el terrorismo, tal como, por otra parte, ha procurado hacer la DEA con los HIDTA, como fuera señalado.

La coordinación es limitada, habiendo sido el Plan para Compartir Inteligencia Criminal un esfuerzo importante para mejorarla.

Las grandes instituciones nacionales con funciones que incluyen la seguridad pública –FBI, DHS, DEA, ATF– producen inteligencia criminal, pero tales instituciones están volcadas en mayor o menor medida a la seguridad nacional y, por otra parte, su producción de inteligencia criminal está orientada a cumplir las finalidades de las respectivas instituciones.

3.3 Australia

3.3.1 Origen

Australia es una monarquía constitucional, Dominio de la Corona británica, cuyas facultades –limitadas– son ejercidas a través de un Gobernador General, y Gobernadores en los estados locales, contando con un sistema de gobierno parlamentario y federal, con un Primer Ministro y un Gabinete, un Parlamento nacional, y Gabinetes y legislaturas locales.

En materia policial, cada Estado y Territorio tiene una institución policial, contando además el Estado nacional con la Policía Federal Australiana, que además presta el servicio policial en el Territorio de la Capital, ciudad de Canberra, a través de su dependencia Policía del Territorio de la Capital.

Existen otros órganos nacionales australianos con funciones policiales o de seguridad pública, como la Oficina de Inmigración y Protección de Fronteras, el Centro Australiano de Informe de Transacciones y Análisis (AUSTRAC), organismo australiano de inteligencia financiera y de lucha contra el lavado de activos y financiamiento del terrorismo, entre otros.

La inteligencia criminal en Australia surgió como respuesta a la aparición en un país con relativamente bajos índices de criminalidad, del delito organizado y del terrorismo, en las décadas de los 60 y 70.

Un aporte significativo para el desarrollo en Australia de la inteligencia criminal, y especialmente de la inteligencia criminal estratégica, estuvo representado por la creación por el Gobierno Federal en 1973 del Instituto Australiano de Criminología, que constituyó un centro para el desarrollo del pensamiento sobre el delito, que influiría en el posterior desarrollo de la inteligencia criminal.

También destacamos la creación en 1977 de la Oficina de Evaluaciones Nacionales, a través de la sanción de la Ley de Evaluaciones Nacionales de 1977, procurándose a través de ella el desarrollo de un pensamiento estratégico, y realizándose evaluaciones estratégicas de información.

En 1981 tuvo lugar la creación de la Oficina Australiana de Inteligencia Criminal (ABCI), establecida a través de un acuerdo administrativo entre el Estado Nacional, los Estados locales y el Territorio del Norte, con la finalidad de establecer un órgano de inteligencia criminal. Este órgano de análisis recibía información de las policías federal y locales, la analizaba, y la suministraba a las instituciones policiales respectivas.

En 1984 fue sancionada la Ley de la Autoridad Nacional sobre el Delito y creación de la Autoridad Nacional sobre el Delito. Esta última constituyó un organismo de inteligencia criminal con facultades de investigación criminal, que incluían la fijación de audiencias y la citación compulsiva de testigos, la interceptación de comunicaciones, la contratación de consultores y asesores, etc.

También debe destacarse la importancia para la asistencia en la formulación de políticas, de la Conferencia Australasiana de Comisionados de Policía, órgano de estudio y asesoramiento en materia policial organizado en 1991/1992, agrupando a diversos órganos de estudios policiales y forenses de Australia y Nueva Zelandia

En 1993 fue creada la Oficina de Evaluaciones Estratégicas del Delito (OSCA) dependiente del Departamento del Attorney General nacional dedicado a la elaboración de inteligencia criminal estratégica.

3.3.2 La ACIC

Finalmente se optó por una organización que en buena medida sintetizara todas las anteriormente descriptas, con el nombre de Comisión Australiana sobre el Delito (ACC) por la Ley de la Comisión Australiana sobre el Delito, 2002.

La ACC absorbió a sus predecesoras NCA, ABCI y OSCA, iniciando su actividad en 2003.

Su denominación, cambió el 1 de Julio de 2016, al incorporar a Crim-Trac, agencia del Departamento del Attorney General nacional de Australia (Ministro con facultades en materia de justicia y seguridad), pasando a denominarse Comisión Australiana de Inteligencia Criminal (ACIC). En 2016 fue asimismo reformada su ley de creación.

Otro aspecto a tener en cuenta fue la sanción de la Ley de la Oficina de Inteligencia Nacional de 2018, que transformó a la nombrada Oficina Nacional de Evaluaciones, en la Oficina de Inteligencia Nacional (ONI) *órgano de inteligencia estratégica al que se asignó*, además, la función de liderar la comunidad de inteligencia nacional, y de evaluar las funciones de las agencias que componían dicha comunidad.

La ley, por otra parte, definió el concepto de comunidad de inteligencia otorgándole una amplitud mayor al que poseía hasta el momento, incluyendo expresamente a la *ACIC,* a la que asignó el carácter de *agencia de inteligencia.*

Lo cierto que la ACIC ha pasado a constituir un organismo de inteligencia pleno, sin por ello perder su carácter de órgano de vinculación entre los sistemas de seguridad pública y de inteligencia.

En lo relativo a las características fundamentales de la ACIC*,* cabe señalar que es un organismo de inteligencia criminal, que posee también funciones especializadas de investigación criminal.

3.3.3 Funciones de la ACIC

Entre las funciones de la ACIC, previstas en su ley de creación se cuentan:

- Obtener, correlacionar, analizar y diseminar información e inteligencia criminal, y mantener una base de datos de tal información e inteligencia;
- Llevar a cabo, cuando fuera autorizada por la Junta, operaciones de inteligencia;
- Investigar, cuando fuera autorizada por la Junta, asuntos relativos a actividad criminal federalmente relevante;
- Conducir o participar en operaciones de integridad relativas al personal de la ACIC, o asistir a la Policía Federal Australiana, al Departamento de Inmigración y Protección de Fronteras o a la Comisión Australiana para la Integridad del accionar policial, a realizar operaciones de integridad;
- Proveer evaluaciones de inteligencia criminal estratégica, o cualquier otra información e inteligencia, a la Junta;
- Proveer asesoramiento a la Junta sobre prioridades nacionales de inteligencia;
- Proveer sistemas y servicios relativos a información nacional policial y proveer chequeos nacionalmente coordinados de historia criminal relativas a un delito federalmente relevante...

La inteligencia criminal suministrada por la ACIC tiene, según el ACIC Corporate Plan 2022/2023, entre sus prioridades el ciberdelito, el delito financiero, las pandillas, el delito grave y organizado de mayor riesgo, las drogas ilícitas y las armas de fuego ilícitas.

Un aspecto de interés de la labor de la ACIC en materia de inteligencia criminal es la identificación de blancos criminales de alto riesgo, representado por las organizaciones criminales de mayor capacidad de daño, tanto nacionales como regionales.

Entre las funciones de la ACIC se cuenta la de apoyar a las instituciones policiales de Australia con *sistemas de información policiales,* a los cuales acceden 76.000 oficiales de policía y otros usuarios acreditados (ACIC Corporate Plan 2022/2023).

Esto incluye información sobre personas de interés, vehículos, armas de fuego y huellas balísticas; servicios biométricos y forenses, incluyendo AFIS (comparación en línea de huellas digitales) y DNA (identificación por comparación de DNA); sistemas de protección destinados a asistir a la policía a encontrar información sobre órdenes de violencia doméstica, delincuentes sexuales dedicados a niños, e identificación de imágenes de explotación

en niños; y sistemas de inteligencia criminal, destinados a facilitar la diseminación y el intercambio de inteligencia criminal entre la ACIC, las policías australianas y otros usuarios acreditados, incluyéndose bases de datos de inteligencia, destacándose el NCIS (Sistema Nacional de Inteligencia Criminal) plataforma informática de inteligencia criminal de intercambio y trabajo en inteligencia criminal entre la ACIC, las policías australianas y otros usuarios autorizados.

Los servicios suministrados por la ACIC al sistema de seguridad pública australiano incluyen los servicios *de* chequeo prestados por el NPCS (Servicio Nacional Policial de Chequeo) a través de los cuales examina la idoneidad de los solicitantes de empleo a órganos policiales, de seguridad, solicitantes de ciudadanía australiana, de los aspirantes a puestos sensibles en materia de seguridad o de confianza, o con acceso a información clasificada. Esta función incluye la emisión, por parte de la ACIC, de evaluaciones de inteligencia criminal.

Otro aspecto significativo de las facultades de la ACIC es la facultad de realizar investigaciones en casos autorizados por la Junta*,* con facultades coercitivas, similares a las de una Comisión Real, las que incluyen que los examiners*,* abogados investigadores de la ACIC, estén facultados para citar a testigos con la fuerza pública de ser necesarios e interrogarlos y requerirles la presentación de documentos o de cosas.

También la ACIC está facultada para obtener información utilizando medios encubiertos, lo que incluye interceptación de comunicaciones, captación de información por medios técnicos, utilización de informantes, etc. Ello, previo otorgamiento de autorizaciones (warrants) y otros controles –Ombudsman, Inspector de Inteligencia y Seguridad, etc.– según los casos.

Cabe destacar que la ACIC está sujeta a la dirección estratégica de la Junta, que establece sus lineamientos generales y ejerce supervisión, presidida por el Comisionado General de la Policía Federal Australiana, e integrada además por el Secretario del Departamento, el Controlador General de Aduanas, el Jefe de la Comisión Australiana de Valores e Inversiones, el Director General de Seguridad, jefe de la Australian Security Intelligence Organization (ASIO), organismo de contrainteligencia y seguridad interna australiano, el jefe de la policía de cada estado y del territorio del Norte, el Jefe de la Policía del Territorio de la Capital, el Funcionario Jefe Ejecutivo de la ACIC, y el Comisionado de Impuestos.

La Junta autoriza a la ACIC a obtener inteligencia y a realizar investigaciones sobre un delito federalmente importante, a establecer fuerzas de tareas, entre otros actos de importancia,

El Funcionario Jefe Ejecutivo (CEO) es quien ejerce la dirección cotidiana y la administración de la ACIC*.*

Es designado por el Gobernador General en consulta con la Junta y con el Comité Intergubernamental, órgano de supervisión de la Junta y de la *ACIC*, formado por el Attorney General –ministro que ejerce las funciones de justicia y seguridad pública en Australia– y un ministro de cada estado, designado por el Primer Ministro de ese estado.

Se desempeña por el término establecido en el instrumento de designación, que no puede exceder de cinco años, siendo un cargo de dedicación exclusiva. Puede cesar en cualquier momento, si el Gobernador General considera insatisfactorio su desempeño, o por incapacidad, quiebra, u otras causas establecidas en la ley.

La actual CEO de la ACIC es Heather Cook, profesional de inteligencia de carrera que se desempeñara en la ASIO (Organizaciòn Australiana de Inteligencia de Seguridad). Su predecesor, March Phelan, fue un oficial de policía de distinguida trayectoria en la Policía Federal de Australia, en la que fue Jefe de la Policía del Territorio de la Capital.

Resulta de interés el rol de los examinadores, que son funcionarios de la ACIC, abogados experimentados que realizan investigaciones (examinaciones) para una investigación u operación especial.

Están facultados para solicitar información de las agencias nacionales, y también de aquellas agencias provinciales que hubieran acordado ello con el Estado Nacional; a citar y a hacer comparecer en forma obligatoria a testigos, y requerir de estos o de otras personas respuestas, documentos relevantes para la investigación, u otras pruebas.

Los examinadores son designados por el Gobernador General, quien debe consultar la designación con el Comité Intergubernamental.

Se trata de una función muy importante, que suele ser ejercida por un número muy reducido de personas[26].

Entre el personal de la ACIC, cabe referir que el organismo puede adscribir a miembros de la Policía Federal Australiana, a otros empleados del Estado Nacional y, por acuerdos con Estados locales, a miembros de policías estaduales o a empleados de los Estados locales. También puede designar otros empleados, así como a consultores.

La ACIC cuenta asimismo con los servicios de analistas de inteligencia, formados en diversas profesiones.

El personal de la ACIC no tiene, en principio, identidad secreta sin perjuicio de que pueden ser autorizados para asumir una identidad secreta para realizar investigaciones u obtener información, en relación a casos de presunto delito grave y organizado, o bien en roles de apoyo con tal finalidad, o en roles de entrenamiento.

El personal de la ACIC está sujeto a un amplio examen preempleo tendiente a establecer eventuales riesgos y vulnerabilidades para la seguridad que pueda representar. Por otra parte, durante su desempeño está sujeto a monitoreo y controles tendientes a prevenir y evitar tales riesgos y vulnerabilidades,

Su personal comprende aproximadamente un millar de personas, incluyendo a unos trescientos adscriptos.

---

26 ACIC, 2020/2021 Annual Report, Commonwealth of Australia, Canberra, 2021, p. 81 (En Línea) Consultado el 14 de mayo de 2024. Disponible en: https://www.acic.gov.au/sites/default/files/2021-10/2020-21%20ACIC%20Annual%20Report%20FULL_0.pdf

La ACIC puede requerir los conocimientos y recursos de las fuerzas policiales estaduales y territoriales, como asimismo recurrir a agencias del Commonwealth, tales como: Policía Federal Australiana, Aduanas, Comisión Australiana de Valores e Inversiones (ASIC), ASIO (organismo de contrainteligencia y seguridad interna). Todas estas agencias están representadas en la Junta de la ACIC.

3.3.4 Controles

En materia de controles, la ACIC cuenta con una auditoría interna dependiente directamente del *CEO,* y con una Comisión de Auditoría independiente, que comparte con el Instituto Australiano de Criminología (AIC).

En materia de control parlamentario, la ACIC está sujeta a un doble control, por comisiones de seguridad pública y de inteligencia.

Cabe destacar que la Comisión Parlamentaria Conjunta sobre Seguridad Pública*,* está facultada para la supervisión y revisión del desempeño y las funciones de la ACIC y de la Policía Federal Australiana (AFP), e informar sobre cualquier asunto relativo a la ACIC y la AFP o su desempeño, del cual la comisión considere que el parlamento debe ser consciente, entre otros aspectos.

También la ACIC está sujeta, bien que en una forma algo más limitada que respecto de los organismos de inteligencia de seguridad nacional, al control del Inspector General de Inteligencia y Seguridad (IGIS).

En materia de formación y perfeccionamiento del personal, la ACIC encara la formación en inteligencia a través de una Vía Básica de Capacitación en Inteligencia Criminal, a través de la cual se procura desarrollar profesionales de inteligencia criminal tanto en roles de obtención de información como en análisis de inteligencia, formación que comprende tanto al personal que se incorpora, como a aquel que ya forma parte del organismo, a lo largo de su carrera.

También la ACIC está comprendida dentro de la jurisdicción de control del Ombudsman de Australia*,* conforme a lo dispuesto en la Ombudsman Act 1976 (Ley del Ombudsman de 1976) y sus leyes modificatorias.

Asimismo, la ACIC está comprendida dentro de la jurisdicción de control de la Comisión Australiana de Integridad en Seguridad Pública (ACLEI) establecida por la Law Enforcement Integrity Commissioner Act 2006.

También la circunstancia de depender la ACIC del Attorney General*.* Tal dependencia constituye otra fuente de control y supervisión para la ACIC.

Otra característica significativa de la ACIC es la cercana relación que mantiene con el Instituto Australiano de Criminología (AIC), instituto de investigación y conocimiento en materia de delito y justicia penal, establecido por la Ley de Investigación Criminológica de 1971.

En el Plan Corporativo 2015 de la entonces *ACC* se proponía la incorporación de la AIC. Ello no se ha concretado hasta el momento, pero se ha mantenido una fuerte relación de cooperación que ha llevado a que ambos organismos compartan personal y conduccio-

nes, manteniéndose no obstante la existencia autónoma y características académicas del AIC, cuya labor ha también contribuido a fortalecer las capacidades de la ACIC.

3.3.5. El ACIM

Asimismo, es preciso destacar que Australia, de modo similar –aunque no idéntico– al Reino Unido, ha procurado desarrollar una doctrina de inteligencia criminal realizando un Modelo Australiano de Inteligencia Criminal (ACIM).

Si bien no ha llegado a nuestras manos –probablemente por estar clasificado– es dable advertir sus características a través de documentos como la Estrategia Australiana de Administración de Inteligencia Criminal 2017/2020[27].

De dicho documento surge que el ACIM estaba en una etapa inicial en su desarrollo. Influyendo verosímilmente en tal circunstancia el carácter federal de Australia, y la inexistencia de normas legales que establezcan la facultad de la ACIC y de la Junta de ésta para establecer normas obligatorias respecto de la producción de inteligencia por parte de las agencias policiales de los estados y territorios, por lo que se ha recurrido a una construcción colectiva, sobre la base del consenso y el peso institucional de la ACIC, de la Junta de ésta, presidida por el Comisionado Jefe de la Policía Federal Australiana (AFP), y de esta última.

Cabe señalar, en primer lugar, que como surge de la Estrategia el Comité Nacional de Capacidades de Inteligencia Criminal (NCICC) es el órgano responsable para la supervisión y la implementación del ACIM y de la Estrategia, integrado por la ACIC, por las policías australianas y por los otros organismos australianos con funciones de seguridad pública, así como por la ASIO, organismo de inteligencia de seguridad australiano.

En el capítulo de la Estrategia "El paisaje de inteligencia criminal de Australia"[28] se señaló, en primer lugar, que una adecuada fotografía de la criminalidad en Australia dependía del entendimiento por parte de los tomadores de decisiones de todos los niveles de la importancia de compartir inteligencia para ayudar en la identificación de amenazas, vulnerabilidades y prioridades, sirviendo la inteligencia como una ventaja para la decisión.

Fue señalada en tal sentido la posibilidad de utilizar tecnología, cultura, e iniciativas de política y legislativas para empoderar el intercambio de información en y alrededor de los puntos de intersección de los dominios señalados, y que desarrollando tales elementos habilitadores, el ACIM y la Estrategia asociados a él podrían suministrar un marco estándar, a través de la administración del ciclo de la inteligencia.

En suma, el ACIM aparece como inspirado en los mismos principios que caracterizan a otras doctrinas nacionales de inteligencia criminal como el NIM: estándares, buenas prácticas, normas y procedimientos comunes a todos los órganos participantes en inteligencia criminal, para trabajar de modo eficazmente coordinado, perfeccionándose y profesionalizándose de forma constante, en búsqueda de la eficiencia y la eficacia en la materia.

---

27 Australian Criminal Intelligence Management Strategy 2017–20 ACIC, Canberra, 2020. (En Línea) Consultado el 14 de mayo de 2024. Disponible en https://www.afp.gov.au/sites/default/files/PDF/ACIM-strategy-2017-20.pdf

28 Ibid. p. 2.

3.3.6 Conclusiones

En definitiva, creemos que continuará el adecuado desarrollo de este interesante organismo y, por otra parte, que la construcción por consenso del *ACIM* habrá de demandar esfuerzos, avances y retrocesos, como, según veremos, sucede en Canadá, pero que prevalecerán las ventajas ínsitas en sumar esfuerzos contra el delito.

3.4 Canadá

3.4.1 Orígenes

Canadá es un Estado de sistema parlamentario, federal, Dominio de la Corona británica, en el que de modo similar a Australia, la Corona británica, Jefe de Estado en Canadá, ejerce esta facultad a través de un Gobernador General, asistido por el Consejo Privado de la Reina para Canadá, y por medio de un Gabinete presidido por un Primer Ministro, elegido por el Parlamento, quien como Jefe de Gobierno encabeza la gestión cotidiana de los asuntos públicos que realiza el Gabinete.

Asimismo, cada una de las provincias cuenta con un teniente-gobernador que ejerce en la provincia un rol equivalente al propio del Gobernador General, y con una legislatura provincial, a cargo del rol legislativo.

Canadá tiene un sistema policial con significativas peculiaridades.

La institución policial fundamental de Canadá es la Royal Canadian Mounted Police -RCMP (Real Policía de Canadá).

La RCMP es la policía nacional y federal de Canadá. Pero al propio tiempo es, por contrato, la policía estadual en diez de los doce estados locales de Canadá, y, también por contrato, en diversos municipios canadienses.

Como policía federal, la RCMP se ocupa de asuntos policiales federales tales como delito grave y organizado y delito financiero. Presta asimismo servicios policiales especializados como el Programa Canadiense de Armas de Fuego y el Centro Nacional de Coordinación contra la Explotación de Niños. Existen además diversas agencias nacionales con funciones que poseen vinculación con la seguridad pública, así como tres instituciones policiales provinciales, y múltiples policías municipales.

En Canadá, entre policías nacionales, provinciales, municipales, tribales y especiales, hay más de cuatrocientas agencias policiales y con funciones policiales.

También es evidente que más allá del desbalance existente en funciones, número de integrantes, presupuesto y capacidades entre la RCMP y las restantes agencias, la inteligencia criminal debe contar en lo posible con todas. De allí que el organismo canadiense de inteligencia criminal, el CISC, cuente en su seno con la casi totalidad de tales agencias, pese a que, como se verá, la integración por parte de una agencia policial del CISC es voluntaria.

Canadá cuenta con tempranos antecedentes en materia de inteligencia criminal derivados de la necesidad de enfrentar la presencia y actuación de organizaciones criminales como la ‘Ndrangheta calabresa, la Familia Rizzuto de Montreal y sus sucesoras, la camorra napolitana, la Sacra Corona Unita de Apulia, Tríadas de China, la Cosa Nostra ítalo-estadou-

nidense, la Yakuza japonesa, etc., así como las bandas de motociclistas (outlaw motorcycle groups), etc.

El 24 de octubre de 1961[29] tuvo lugar una reunión presidida por el Comisionado C.W. Harvison de la Royal Canadian Mounted Poice (RCMP) de la que formaron también parte representantes de la Policía Provincial de Quebec, de la Policía de Montreal, y de la Policía Metropolitana de Toronto, donde se acordó el establecimiento de una agencia central para la distribución de inteligencia criminal, y que tal rol debía ser asumido por la RCMP.

Tras una serie de reuniones con participación de funcionarios nacionales y provinciales, y la creación de comisiones, para materializar y canalizar ayuda del Gobierno Federal para la lucha contra el delito, en la Conferencia Federal-Provincial sobre Delito Organizado celebrada el 5 y 6 de enero de 1966 se dispuso la creación de una comisión formada por funcionarios policiales, denominada Comisión de inteligencia sobre el Delito, que el 8 de agosto de 1967 presentó su informe al Fiscal General del Estado y a los Procuradores Generales provinciales, recomendando la creación de un nuevo mecanismo central de inteligencia, a llamarse Sistema Canadiense de Inteligencia sobre el Delito.

Se propuso que el nuevo Sistema tuviera un repositorio central en Ottawa, a denominarse Centro Nacional de Inteligencia sobre el Delito, y que se establecieran centros provinciales de inteligencia sobre el delito en cada una de las provincias.

Se planteó que el Centro Nacional recibiera, registrara y diseminara inteligencia recibida de los Centros Provinciales y de toda otra fuente, y que los Centros Provinciales llevaran a cabo funciones similares dentro de sus respectivas jurisdicciones.

3.4.2 El CISC

En la reunión, se adoptó la denominación Servicio de Inteligencia Criminal de Canadá (CISC), resolviéndose mantener una oficina central en Ottawa administrada por la RCMP, acordándose estar un sistema de oficinas provinciales o regionales sujeto a la dirección de un Comité Ejecutivo, el que designaría a un Director del CISC, así como a un Director Asistente.

En la segunda reunión del Comité Ejecutivo del CISC, el 5 de marzo de 1970 en Rockliffe, Ontario, fue adoptado el Manual de Procedimientos del CISC, acordándose además adoptar la Constitución del CISC.

El 7 de diciembre de 1976 se convocó una reunión especial del Comité Ejecutivo del CISC en Ottawa, para considerar la propuesta de adopción del Sistema Automatizado de Información de Inteligencia Criminal (ACIIS), para el uso restricto de inteligencia criminal por parte de la comunidad policial canadiense, lo que así se resolvió.

En definitiva, podemos advertir que el CISC nació como una construcción colectiva entre el Ministerio Público –fiscales– nacionales y provinciales de Canadá, por una parte, y

29 En cuanto a la historia de la conformación del CISC, constituye nuestra fundamental referencia de, CISC, The History of Criminal Intelligence Service Canada, Ottawa, 1988.(En Línea) Consultado el 14 de mayo de 2024. Disponible en: https://www.publicsafety.gc.ca/lbrr/archives/hv%208079.o73%20h58%201978-eng.pdf

las instituciones policiales canadienses, presididas por la RCMP por la otra, para enfrentar y superar el desafío representado por el delito organizado en Canadá, y que se materializó en una organización voluntaria formada por policías y organismos con funciones policiales.

El CISC no constituyó un organismo creado por ley, como en otros casos examinados, sino que surgió de una constitución votada y consensuada entre sus miembros.

El CISC está constituido sobre la base, y con claro predominio, de la Real Policía Montada de Canadá (RCMP), institución policial fundamental de dicho país, con facultades de policía federal, policía estadual en ocho de las diez provincias canadienses, y policía municipal por contrato en 199 municipios.

La integración del CISC comprende, además de la RCMP*,* a las instituciones policiales provinciales e instituciones policiales locales, así como a organismos públicos que, aunque no poseen directamente facultades policiales, brinda servicios a instituciones policiales. También pueden excepcionalmente ser admitidas instituciones o agencias extranjeras, si se considera que ello es en beneficio de la comunidad de inteligencia criminal.

Conforme a la constitución del *CISC,* constituye su finalidad:…unir a la comunidad canadiense de inteligencia criminal en los niveles municipales, provinciales y federales, para combatir el delito más efectiva y eficazmente… (art. 1º).

De acuerdo al artículo 2°, el mandato del *CISC* es el de:

…ser una organización estratégicamente enfocada, que asegura la producción e intercambio oportunos de información e inteligencia criminal entre las agencias miembros del CISC y el de ser un 'centro de excelencia' nacional para apoyar el esfuerzo nacional para detectar, reducir, desorganizar y prevenir el delito serio y organizado que afecte Canadá…

Posee una Oficina Central en Ottawa, y una red de Oficinas Provinciales.

La Oficina Central tiene a su cargo entre otros aspectos, sobre la base de la información y la inteligencia criminal que recibe de las instituciones policiales y las Oficinas Provinciales, la elaboración de los productos de inteligencia criminal nacionales. De ella depende, además, el Sistema Automatizado de Inteligencia Criminal, fundamental para el intercambio de información e inteligencia.

El personal de la Oficina Central comprende personal de la RCMP y personal adscripto de otras instituciones policiales canadienses, siendo su apoyo administrativo, logístico y financiero provisto por la RCMP.

El CISC está dirigido por un Comité Ejecutivo, presidido por el Comisionado de la RCMP y formado por representantes de las instituciones policiales miembros, con predominio de la RCMP.

También cuenta con un Comité Supervisor, con la función de asistir al Director General del CISC para cumplir el Mandato del órgano e implementar las decisiones alcanzadas por el Comité Nacional Ejecutivo (art. 22). Formado por los Directores de las Oficinas Provinciales, el Director General del CISC, y los Vicedirectores Generales *de la* Oficina Central, bayo la presidencia del Director General del CISC.

Cada Oficina Provincial recibe información de las instituciones policiales de la provincia, y suministra inteligencia criminal a la Oficina Central.

Cada Oficina Provincial posee cierta autonomía, pero debe observar los estándares de servicio comunes establecidos en el CISC.

La pertenencia al CISC se adquiere y pierde por decisión de las Oficinas Provinciales. Requiere el compromiso por parte de la institución miembro de asistir a las reuniones correspondientes, de someter detallados y oportunos informes de inteligencia, participar en las funciones de adiestramiento de su Oficina Provincial, contribuir a la base de datos nacional de inteligencia criminal del CISC, y participar en la obtención e intercambio oportuno de información e inteligencia criminal.

A cambio de ello, el miembro accede a la base de datos conforme a su categoría, y se beneficia de la capacitación brindada en el seno del CISC.

3.4.3 El CCIM

Cabe señalar que el CISC, la RCMP y la Canadian Association of Chiefs of Police (Asociación Canadiense de Jefes de Policía – CACP) han elaborado, a semejanza del Reino Unido, un Modelo Nacional Canadiense de Inteligencia Criminal (CCIM).

A pesar de la limitada difusión que es hecha en el ámbito académico de este Modelo y de los productos de inteligencia elaborados conforme a él, con las excepciones que se indicarán, recurriendo a las fuentes disponibles, habremos de establecer sus aspectos fundamentales.

El primero consistía en la entrega de productos y servicios de inteligencia, para lo cual el CCIM establecía estándares aceptados en todo el país a través de productos de inteligencia principales, como las evaluaciones integradas de amenaza provinciales y nacional, evaluaciones estratégicas y tácticas, y evaluaciones de alerta temprana estratégicas, como Sentinels y Watch List.

El segundo pilar refería a la guarda, recuperación e intercambio de información e inteligencia, para lo cual se preveía que el CCIM establecería procesos y protocolos para identificar y priorizar críticas lagunas de inteligencia, estrategias de obtención de información, y procedimientos de comunicación, para asistir a la actividad policial para encarar lagunas críticas de conocimiento y mitigar amenazas y riesgos, mientras se aseguraba el suministro de información e inteligencia oportunos entre todos los miembros del CISC, a través de Canadá.

El tercer pilar, asignación de tareas, coordinación y aplicación, se refiere a que el CCIM requiere que los procesos de toma de decisiones estratégicos y operacionales sean guiados por la inteligencia, y que los productos analíticos tanto informen, como conduzcan la asignación de tareas. Se señaló que esto proveería tanto el marco, como la información para alinear recursos con prioridades y para revisar estas últimas a la luz de amenazas o tendencias emergentes.

Se señaló que un componente importante de este pilar era el control de calidad o mecanismo de auditoría, para medir el valor y la eficacia del proceso de inteligencia, y de los productos realizados.

El cuarto pilar, la profesionalización de la función de inteligencia, derivó de la circunstancia de que el enfoque del CCIM de apoyar la actividad policial guiada por la inteligencia (intelligence-led policing), trajo consigo un énfasis renovado en la exigencia de mayor profesionalismo, entrenamiento constante y desarrollo de especialistas en inteligencia.

Fue señalado que eran principios claves del *CCIM* la incorporación de buenas prácticas y de herramientas que ya estaban funcionando, como la técnica Sleipnir de evaluación de amenaza, la Escala de Priorización del Daño, y las evaluaciones de amenaza nacional y provinciales.

Cabe señalar que el Comité Ejecutivo Nacional (NEC) del CISC, adoptó en marzo de 2006 la decisión de apoyar el desarrollo del CCIM, decisión seguida de procesos de inicio en 2007 y 2008[30].

Cabe destacar que *la* Asociación Canadiense de Jefes de Policía (CACP*)* aprobó la Resolución Nº 08-2008[31], Apoyo para el Modelo Canadiense de Inteligencia Criminal (CCIM), recomendando que todos los miembros de la Asociación en Canadá apoyaran plenamente los esfuerzos del Equipo de Proyecto del CCIM para desarrollar un detallado Plan de Proyecto, Declaración Objetiva y Caso de la Profesión, para asegurar la implementación exitosa del Modelo, para alinear estratégicamente inteligencia y operaciones en los niveles municipal, provincial y federal a través de Canadá.

En 2008, y como consecuencia de decisiones adoptadas por el NEC del CISC y la Asociación Canadiense de Jefes de Policía (CACP), comenzó un período de amplias consultas con los interesados entre mayo y noviembre del año referido, que llevó a identificar estándares y procesos claves para la implementación del CCIM[32].

Conforme al CISC[33], el Modelo Canadiense de Inteligencia Criminal es un proceso de extremo a extremo para gerenciar e integrar eficazmente la actividad policial en todos los niveles del cumplimiento de la ley a través de Canadá: municipal, provincial, federal e internacional.

Se señaló que la Oficina Central del CISC tenía a su cargo la coordinación e implementación del CCIM, con amplia consulta de la comunidad de inteligencia criminal y, más ampliamente, de la comunidad de seguridad pública.

---

30 WALSH, Patrick F. Intelligence and Intelligence Analysis, Routledge, London, 2011, p. 202.

31 CACP. Resoluciones dictadas en la 130ª Conferencia Anual, Montreal, Quebec, agosto de 2008. (En Línea) Consultado el 14 de mayo de 2024. Disponible en: https://www.cacp.ca/_Library/resolution/20140805142505143830140 5_resolutionsadopted2009.pdf

32 WALSH, Patrick F. Op. Cit. pp. 202-203.

33 Criminal Intelligence Service Canada, Integrated Threat Assessment Methodology, Version 1.0, Ottawa, 2007, pp. 15-16.

En 2011 se escribía en una obra de interés[34], respecto del CCIM que a diferencia de su equivalente inglés, estaba aún en una fase de desarrollo[35]. A pesar del tiempo transcurrido desde que esta observación se efectuaba, creemos por las razones que se indicarán, que es difícil que haya alcanzado un desarrollo similar al inglés, dada la circunstancia de ser el CISC un organismo de inteligencia criminal de desarrollo y capacidades evidentemente inferiores al NCIS-SOCA-NCA británico.

Por otra parte, en el artículo en comentario se reconoció que las agencias policiales en Canadá tenían diferentes enfoques en materia de formación y entrenamiento de analistas y en materia de elaboración de productos de inteligencia. Cabe recordar en este aspecto que la estandarización de productos de inteligencia para facilitar su intercambio tanto horizontal como entre los diversos niveles es uno de los aspectos fundamentales del NIM.

Entre los desafíos que fueron señalados para la plena implementación del CCIM, destacamos que Canadá, como Estado federal, no podía, a diferencia del Reino Unido, legislar a nivel nacional para cambiar los estándares policiales, dado que la policía era responsabilidad de las provincias[36].

De ese modo, aunque todos los jefes policiales habían aprobado el concepto del CCIM, su implementación constituiría una etapa posterior que se habría de mostrar desafiante, destacándose que el equipo de implementación del proyecto no podía, desde los cuarteles generales de la RCMP en Ottawa, obligar a una agencia a implementar el Modelo. NEC del CISC tendría un rol importante en la implementación.

Debemos señalar que a partir de 2014 no hemos podido obtener en Internet nueva información sobre el CCIM, lo que permite conjeturar que no ha sido posible avanzar en su implementación. Hemos efectuado directamente una consulta por correo electrónico al CISC, la que hasta el momento no ha sido respondida.

Lo expuesto no implica desconocer los logros de Canadá en materia de inteligencia criminal. Habremos pues de referir otros aspectos relativos a la materia en este país.

En Canadá es relevante la Asociación Canadiense de Jefes de Policía, organización de ejecutivos de policía de Canadá de intercambio de ideas y cabildeo en beneficio de las instituciones que representan, y de la seguridad pública en el país, que funciona como foro de propuesta y debate de la comunidad policial canadiense para el perfeccionamiento técnico y ético de la actividad policial.

Del trabajo en común entre el CISC y la CAPC surgieron interesantes desarrollos doctrinarios como la Metodología de Evaluación Integrada de Amenazas (ITAM), surgido de la experiencia de la producción por parte de la Oficina Central del CISC de la primera Evaluación Nacional de la Amenaza del Delito Grave y Organizado en Canadá, documento fundamental de inteligencia criminal canadiense en 2003, que pasó a derivar en un plan nacional

34 WALSH, Patrick F. Loc. Cit.

35 Ibid. p. 200.

36 Ibid. pp. 207-208.

de obtención de información criminal, y en reuniones de un grupo de trabajo de nivel nacional, destinado a establecer estándares analíticos para las evaluaciones[37].

En 2007 se destacaban como productos de análisis de inteligencia criminal estratégica elaborados por el CISC, la Evaluación Nacional de la Amenaza del Delito Grave y Organizado en Canadá, documento anual destinado a asistir en la toma de decisiones por parte de los jefes policiales en Canadá, así como a proveer una evaluación general de alcance nacional para la comunidad canadiense de inteligencia criminal.

Asimismo, la Estimación Nacional Criminal de Inteligencia sobre el Delito Grave y Organizado tiene la finalidad de suministrar una visión general de tales amenazas en Canadá, para posibilitar la toma informada de decisiones por parte de altos funcionarios gubernamentales

El Informe Anual sobre Delito Organizado en Canadá, el único informe público sobre esta materia elaborado por órganos de cumplimiento de la ley en Canadá, es publicado con la finalidad de informar y educar al público sobre los efectos de las aludidas amenazas y el modo cómo afectan a Canadá.

3.4.4 Conclusiones

En suma, Canadá cuenta con un organismo de inteligencia criminal, que vincula a la gran mayoría de las instituciones canadienses con funciones policiales, con interconexión telemática y diversos avances hacia una doctrina de inteligencia criminal común,

Mientras resulta evidente la importancia lograda por el CSIS en la seguridad pública de Canadá, también cabe advertir que se trata de un órgano establecido por una Constitución surgida de un convenio entre las múltiples instituciones policiales que lo conforman, en torno a la RCMP, que constituye la base y el soporte administrativo del CISC.

La falta de legislación determina el carácter imprescindible del consenso, circunstancia que parece poner un límite a la plena adopción de una doctrina de inteligencia criminal común, como el CCIM.

De todos modos, el CSIS parece haber sido de fundamental importancia para poner al alcance de las múltiples policías locales los recursos, la información y la inteligencia criminal de la RCMP y de las restantes policías locales y, al propio tiempo, asegurar que la información de las más remotas policías locales llegue a la RCMP y a las restantes. Aunque la integración al CSIS es voluntaria, los evidentes beneficios determinan que la casi totalidad de las policías locales acepten las obligaciones que tal membresía impone, particularmente en lo relativo al suministro de información e inteligencia criminal.

37 Criminal Intelligence Service Canada (CISC). Loc. Cit.

4. Apuntes sobre la inteligencia criminal en Latinoamérica

Nos proponemos realizar en esta revista un estudio sobre la inteligencia criminal en Latinoamérica, tema sobre el que ya hemos realizado aportes[38].

Destacamos que bajo diversas denominaciones –inteligencia policial, inteligencia de seguridad pública, inteligencia criminal, análisis del delito– la inteligencia criminal es practicada en Latinoamérica.

Tres países de la región cuentan con organismos de inteligencia criminal: Argentina, la Dirección Nacional de Inteligencia Criminal (DNIC) del Ministerio de Seguridad; Brasil, la Dirección de Operaciones Integradas y de Inteligencia (DIOPI) dependiente de la Secretaría Nacional de Seguridad Pública del Ministerio de Justicia y Seguridad Pública; y la Dirección Nacional de Inteligencia Civil (DIGICI) dependiente del Ministerio de la Gobernación de la República de Guatemala.

En el caso de Brasil, elaboró una Doctrina de Inteligencia para la Seguridad Pública, así como vinculó en forma telemática con el órgano central de inteligencia de seguridad pública –hoy la citada DIOPI– a los órganos de inteligencia de seguridad pública de sus instituciones policiales, fuerzas de seguridad, y órganos de conducción de seguridad pública.

En Colombia, la Dirección de Inteligencia Policial de la Policía Nacional (DIPOL) ha logrado un significativo desarrollo técnico y doctrinario, reflejado en su rol de organización de mecanismos de cooperación policial, como CLACIP y AMERIPOL, este último hoy institucionalizado a través de un tratado suscripto por trece de sus países miembros.

Costa Rica, dentro del Organismo de Investigación Judicial, dependiente de la Corte Suprema de Justicia, ha constituido la Oficina de Planes y Operaciones (OPO), y formando parte de ella, la Unidad de Análisis Criminal, organismo de análisis del delito, que apoya la investigación criminal y la inteligencia criminal.

También la Dirección de Inteligencia de la Policía Nacional del Perú (DIRIN) ha logrado un importante desarrollo técnico, al igual que los órganos de inteligencia policial de otras instituciones de la región.

En el caso de Chile, merece destacarse que la Ley N°19974 incluyó dentro del Sistema de Inteligencia de Estado a la inteligencia policial, estableciendo que dicha función corresponde exclusivamente a Carabineros e Investigaciones (Art. 22). Establece, además la citada ley, que esta función comprende el procesamiento de la información relacionada con las actividades de personas, grupos y organizaciones que de cualquier manera afecten o puedan afectar las condiciones del orden público y de la seguridad pública interior.

38 Así, de UGARTE, José Manuel. "Panorama de la inteligencia criminal latinoamericana. Desarrollo, dilemas y dificultades", Revista electrónica URVIO, N° 15, 2014, Flacso Andes, Quito, DOI: https://doi.org/10.17141/urvio.15.2014.1586 ; "Desarrollo, situación y probable evolución de la inteligencia criminal en Latinoamérica", ALACIP, 2019, obtenido en https://alacip.org/cong19/285-ugarte-19.pdf ; "La inteligencia criminal en Argentina y Brasil", capítulo 1 del libro "Teoria e práticas de Inteligência de Segurança Pública" Editora Plácido, Belo Horizonte, entre otros.

Consiguientemente, reservada de ese modo la referida función de inteligencia policial al Departamento de Inteligencia de Carabineros y la Subdirección de Inteligencia, Crimen Organizado y Seguridad Migratoria de la Policía de Investigaciones, tras la creación del Ministerio del Interior y Seguridad Pública fue creado el Centro Estratégico de Análisis del Delito, hoy Centro de Estudios y Análisis del Delito (CEAD) órgano de análisis del delito, que basándose en estudios, estadísticas e información territorial, apoya la formulación, monitoreo y evaluación de las políticas públicas de seguridad interior.

5. CONCLUSIONES

Del análisis efectuado en el presente, surgen las características fundamentales de la inteligencia criminal y de su aplicación en aquellos países en los cuales, a nuestro juicio, ha alcanzado mayor desarrollo.

De ello surge el interés que posee como medio fundamental para adquirir conocimiento sobre el delito, y, por consiguiente, estar en condiciones de prevenirlo y de combatirlo con mayor eficiencia y eficacia.

El conocimiento del delito tiene mayor importancia aún cuando se trata de organizaciones criminales trasnacionales, que frecuentemente se caracterizan por el secretismo que procuran establecer sobre sus actividades y características.

En Latinoamérica, como ya se ha referido, son aún pocos países que han procurado organizar y emplear inteligencia criminal.

Latinoamérica, como otras regiones del mundo, registra una significativa presencia de organizaciones criminales trasnacionales.

Por esa razón, es que consideramos útil il que bajo dependencia del ministerio encargado de la seguridad pública exista un organismo de inteligencia criminal, constituido fundamentalmente por los policías mejor formados en inteligencia y con mayor ética en su función, y por analistas sin estado policial, profesionales en disciplinas útiles para conocer el delito, así como buenos técnicos informáticos y personal de apoyo.

Las experiencias mencionadas en este trabajo pueden servir de guía, con la debida adaptación a las características del país en que se resuelva actuar.

REFERENCIAS BIBLIOGRÁFICAS

ACIC, *2020/2021 Annual Report*, Commonwealth of Australia, Canberra, 2021, p. 81 (En Línea) Consultado el 14 de mayo de 2024. Disponible en: https://www.acic.gov.au/sites/default/files/2021-10/2020-21%20ACIC%20Annual%20Report%20FULL_0.pdf

Australian Criminal Intelligence Management Strategy 2017–20 ACIC, Canberra, 2020. (En Línea) Consultado el 14 de mayo de 2024. Disponible en: https://www.afp.gov.au/sites/default/files/PDF/ACIM-strategy-2017-20.pdf

ANDREWS, Paul P., Jr. y PETERSON, Marilyn B., *Criminal Intelligence Analysis,* Palmer Enterprises, Loomis, 1990.

AUMOND, Karen. Tactical and Strategic Intelligence. Issues of Interest to Law Enforcement. Criminal Intelligence. A Vital Police Function. Law Enforcement Intelligence Unit (LEIU), February 1998, pp. 35-36. Citado por MOREHOUSE, Bob. The Role of Criminal intelligence in Law Enforcement en MOREHOUSE, Bob, PETERSON, Marilyn B. y PALMIERI Lisa. (Eds.). "Criminal Intelligence for the 21st century" Law Enforcement Intelligence Units (LEIU) & International Association of Law Enforcement Intelligence Analysts (IALEIA), Sacramento & Richmond, reimpresión, 2017.

BOBA, Rachel. Crime Analysis and Crime Mapping, Sage Publications, Thousand Oaks, 1993.

CACP. (Canadian Association Chiefs of Police). Resoluciones dictadas en la 130ª Conferencia Anual, Montreal, Quebec, agosto de 2008.(En Línea) Consultado el 14 de mayo de 2024. Disponible en: https://www.cacp.ca/_Library/resolution/20140805142505143830 1405_resolutionsadopted2009.pdf

CISC, *The History of Criminal Intelligence Service Canada,* Ottawa, 1988.(En Línea) Consultado el 14 de mayo de 2024. Disponible en: https://www.publicsafety.gc.ca/lbrr/archives/hv%208079.o73%20h58%201978-eng.pdf

GENERAL ACCOUNTING OFFICE. INFORMATION Sharing: Agencies Could Better Coordinate to Reduce Overlap in Field-Based Activities. Informe 13-471 de abril 2013. Fecha de consulta 22 de febrero de 2021. Recuperado el 20 de marzo de 2022. Disponible en: https://www.gao.gov/products/gao-13-471

GORDNIER John. "Legal Issues in U.S. Criminal Intelligence: An Overview", en MOREHOUSE, Bob, PETERSON, Marylin B. and PALMIERI, Lisa (Eds.). "Criminal Intelligence for the 21st Century", IALEIA-LEIU, Richmond, 2019.

HARRIS, Don. "Basic Elements of Intelligence. Revised. Law Enforcement Assistance Administration" Washington D.C., 1976, p. 1.8. Citado por MOREHOUSE, Bob. "The Role of Criminal intelligence in Law Enforcement" en MOREHOUSE Bob, PETERSON, Marilyn B. y PALMIERI, Lisa. (Eds.)." Criminal Intelligence for the 21st century", Law Enforcement Intelligence Units (LEIU) & International Association of Law Enforcement Intelligence Analysts (IALEIA), Sacramento & Richmond, reimpresión, 2017

KESSLER, Ronald. "The FBI", Pocket Books, New York, 1993.

MOREHOUSE Bob, PETERSON, Marilyn B. y PALMIERI Lisa. (Eds.). "Criminal Intelligence for the 21st century" Law Enforcement Intelligence Units (LEIU) & International Association of Law Enforcement Intelligence Analysts (IALEIA), Sacramento & Richmond, reimpresión, 2017.

MOREHOUSE Bob. "The Role of Criminal intelligence in Law Enforcement", en MOREHOUSE, Bob, PETERSON, Marilyn B. y PALMIERI Lisa. (Eds.). "Criminal Intelligence for the 21st century" Law Enforcement Intelligence Units (LEIU) & International Association of Law Enforcement Intelligence Analysts (IALEIA), Sacramento & Richmond, reimpresión, 2017.

MORRIS, Jack. "The Criminal Intelligence File", The Palmer Press, Loomis, 1983.

OSBORNE, Deborah. "Out of Bonds: Innovation and Change in Law Enforcement Analysis", Joint Military Intelligence College, Washington D.C., march 2006

PETERSON, Marilyn B. " Application in Criminal Analysis: A Sourcebook", Praeger, Westport, 1994,

PETERSON, Marilyn B. Analysis and Synthesis, en MOREHOUSE, Bob. "et al". Op. Cit. pp. 88-108.

ANDREWS, Paul P., Jr. y PETERSON, Marilyn B. "Criminal Intelligence Analysis", Palmer Enterprises, Loomis, 1990.

RATCLIFFE Jerry H. "Integrated Intelligcence and Crime Analysis: Enhanced Information Management for Law Enforcement Leaders", Second Edition, COPS-Police Foundation, Washington, 2007

RATCLIFFE, Jerry H. "Intelligence-Led Policing", Willan Publishing, Cullompton, 2008.

UGARTE, José Manuel. "Panorama de la inteligencia criminal latinoamericana. Desarrollo, dilemas y dificultades", Revista electrónica URVIO, N° 15, 2014, Flacso Andes, Quito, DOI: https://doi.org/10.17141/urvio.15.2014.1586.

UGARTE, José Manuel. Desarrollo, situación y probable evolución de la inteligencia criminal en Latinoamérica", ALACIP, 2019. (En Línea) disponible en: https://alacip.org/cong19/285-ugarte-19.pdf

UGARTE, José Manuel. "La Inteligencia Criminal", en DEL PERCIO, Enrique. (comp.) "Prejuicio, Crimen y Castigo", Coppal-Editorial Sudamericana, Buenos Aires, 2010

UGARTE. José Manuel. "La inteligencia criminal en el Reino Unido y en Canadá Primera Parte", en Revista "Policía y Criminalística", Editorial Policial, Nº 16, vol. 362, Buenos Aires, 2005,

UGARTE, José Manuel. "La inteligencia criminal en el Reino Unido y en Canadá, Segunda Parte, El Modelo Nacional de Inteligencia", en Revista "Policía y Criminalística", Editorial Policial, N° 18, Buenos Aires, marzo de 2007.

UGARTE, José Manuel. “La inteligencia criminal en el Reino Unido y en Canadá-Tercera Parte-Canadá”, en Revista “Policía y Criminalística”, Editorial Policial, N° 19, Buenos Aires, 2007.

UGARTE, Jose Manuel, “La inteligencia criminal en Argentina y Brasil”, capítulo 1 del libro “Teoria e práticas de Inteligência de Segurança Pública» Helio Hiroshi Hamada y Renato Pires Moreira, Editora D’Plácido, Belo Horizonte, 2019.

U.S. DEPARTMENT OF JUSTICE, Office of Justice Programs. (En línea) Regional Information Sharing Systems Program. (Fecha de consulta 14 de mayo de 2024). Disponible en: https://www.ojp.gov/pdffiles1/bja/192666.pdf

U.S DEPARTMENT OF JUSTICE, Global Justice Information Sharing Initiative, National Criminal Intelligence Sharing Plan, Washington, 2003.

U.S. DEPARTMENT OF JUSTICE, OFFICE OF THE INSPECTOR GENERAL, June 2005 (En Lìnea) The Department of Justice’s Terrorism Task Forces Evaluation and Inspections Report I-2005-007. (Fecha de Consulta 1 de mayo de 2024). Disponible en: https://oig.justice.gov/reports/plus/e0507/index.htm

U.S. HOUSE OF REPRESENTATIVES. (En Línea) Regional Information Sharing Systems Program (Fecha de consulta 14 de mayo de 2024). Disponible en: https://docs.house.gov/meetings/AP/AP19/20130321/100498/HHRG-113-AP19-Wstate-KennedyD-20130321.pdf

U.S. DEPARTMENT OF JUSTICE, GLOBAL JUSTICE INFORMATION SHARING INITIATIVE. (2003) The National Criminal Intelligence Sharing Plan, p. 14. (En línea) (Fecha de Consulta 1 de mayo de 2024). Disponible en: https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/national_criminal_intelligence_sharing_plan.pdf

WALSH, Patrick F. “Intelligence and Intelligence Analysis”, Routledge, London, 2011

AMENAZAS HÍBRIDAS Y LA POLÍTICA DE DEFENSA NACIONAL DE CHILE *∞

CLAUDIO BERTIN WIEHOFF•

RESUMEN

El presente trabajo de investigación pretende identificar las amenzas híbridas que afectan o podrían afectar a Chile, así como entregar una clasificación de ellas. Del mismo modo presenta la relación que tienen dichas amenazas con la Política de Defensa Nacional y cuál es la influencia que tienen sobre ésta. Para ello es que se ha realizado un análisis de lo establecido por los principales autores que han escrito desde el año 2006, fecha en que se comienza a utilizar y se identifican las amenazas y los conflictos híbridos. Posteriormente se realizó una descripción de las principales amenazas híbridas para luego proceder a su clasificación, según lo establecen los principales centros europeos que se han dedicado a estudiar este tipo de conflictos. Finalmente se realiza una descripción de la Política de Defensa Nacional para determinar cómo se relaciona la estrategia de defensa, las capacidades estratégicas, los objetivos y áreas de misión y la influencia que tienen las amenazas híbridas en ella.

***Palabras clave**: Amenaza híbrida; conflicto híbrido; clasificación de amenazas híbridas; efectos de las amenazas híbridas sobre la Política de Defensa Nacional; Política de Defensa Nacional y las amenazas híbridas.*

HYBRID THREATS AND NATIONAL DEFENSE POLICY OF CHILE

ABSTRACT

This research work aims to identify the hybrid threats that affect or could affect Chile, as well as provide a classification of them. In the same way, it presents the relationship that these threats have with the

---

* El escrito es el resultado del trabajo de investigación presentado a la Academia Nacional de Estudios Políticos y Estratégicos para la obtención del grado de Magíster en Relaciones Internacionales, Seguridad y Defensa actuando como profesor guía el Dr. Ariel Álvarez Rubio.

• Magíster en Relaciones Internacionales, Seguridad y Defensa (ANEPE), Magíster en Planificación y Estrategia en Operaciones Militares Conjuntas (AGA), Máster en Diseño, Gestión y Dirección de Proyectos (UNINI–UEMC), Oficial de Estado Mayor (AGA), Profesor Militar de Academia (ACAPOMIL–APA), Ingeniero Politécnico Militar (ACAPOMIL), Ingeniero en Ejecución en Defensa Aérea (APA), Piloto Comercial (DGAC), especialista en Derecho Internacional Humanitario (DIH) y Género (IIHL). cbertinw@gmail.com. ORCID: https://orcid.org/0009-0005-4011-0364

∞ Fecha de recepción: 270424 - Fecha de aceptación: 260624.

National Defense Policy and what influence they have on it. To achieve this, an analysis has been carried out of what has been established by the main authors who have written since 2006, the date on which it began to be used and threats and hybrid conflicts were identified. Subsequently, a description of the main hybrid threats was made and then proceeded to their classification, as established by the main European centers that have dedicated themselves to studying this type of conflicts. Finally, a description of the National Defense Policy is made to determine how the Defense Strategy, Strategic Capabilities, Objectives and Mission Areas are related and the influence that hybrid threats have on it.

***Keywords**: Hybrid threat; hybrid conflict; hybrid threat classification; effects of hybrid threats on National Defense Policy; National Defense Policy and hybrid threats.*

AMEAÇAS HÍBRIDAS E POLÍTICA DE DEFESA NACIONAL DE CHILE

RESUMO

O Este trabalho de pesquisa visa identificar as ameaças híbridas que *afetam ou podem afetar o Chile, bem como fornecer uma classificação das mesmas. Da mesma forma, apresenta a relação que estas ameaças têm com a Política de Defesa Nacional e qual a influência que nela exercem. Para isso, foi realizada uma análise do que foi estabelecido pelos principais autores que escreveram desde 2006, a data em que começou a ser utilizado e foram identificadas ameaças e conflitos* híbridos. Posteriormente *foi feita uma descrição das principais ameaças* híbridas e posteriormente *procedeu-se à sua classificação, conforme estabelecido pelos principais centros europeus que se têm dedicado ao estudo deste tipo de conflitos. Por último, é feita uma descrição da Política de Defesa Nacional para determinar como se relacionam a Estratégia de Defesa, as Capacidades Estratégicas, os Objectivos e as Áreas de Missão e a influência que as ameaças* híbridas *têm sobre a mesma.*

***Palavras-chave**: Ameaça* híbrida; *conflito* híbrido; *classificação de ameaças* híbridas; *efeitos das ameaças* híbridas na Política de Defesa Nacional; Política de Defesa Nacional e *ameaças* híbridas.

Introducción

Tras el asesinato del archiduque Francisco Fernando de Austria, el 28 de junio de 1914, en Sarajevo, Bosnia, se da inicio a lo que sería el conflicto armado que tuvo como resultado una de las mortandades registradas en el continente europeo más importantes

de todos los tiempos, con algunos cálculos que hablan de más de 31 millones de muertos y donde combatieron más de 70 millones de militares, situación que se generó en un ambiente de gran incertidumbre. Al ser consultado el historiador contemporáneo Charles Seignobos respecto a si creía en la posibilidad de un conflicto generalizado que afectara a las grandes potencias de su tiempo, el citado historiador apoyándose en el progreso y desarrollo cultural y filosófico de Occidente y del peso del intercambio comercial entre los países y de las competencias de los diplomáticos para generar pactos y consensos, negó la posibilidad de que siquiera un conflicto general pudiese afectar a la seguridad de los europeos. Esta experiencia nos enseña la dificultad que existe para poder prospectar los hechos en el ámbito de los conflictos armados[1].

La evolución de los conflictos no ha sido menos compleja en estos días, es así como en la "Política de Defensa Nacional", publicada el año 2020, se plantea que además de las amenazas tradicionales y conflictos interestatales, como los que se ha visto enfrentado nuestro país durante su existencia, se encuentran presentes hoy en día nuevas amenazas denominadas también como "amenazas híbridas", las que pueden tener un origen interno o externo, estatal o no estatal y poseen una alta capacidad de dañar a la población y a la infraestructura crítica del Estado[2]. En atención a lo señalado, es que se genera la inquietud de contar con un panorama actualizado sobre estas amenazas que enfrenta el Estado y que han sido recientemente señaladas por la citada Política de Defensa; para ello es que se requiere identificar y clasificar dichas amenazas, así como determinar cuál podría ser la influencia y el efecto que podrían tener en la Política de Defensa de nuestro país. Si bien es cierto la problemática planteada con relación a las amenazas híbridas es relativamente nueva, existen algunos politólogos y polemológicos que vienen estudiando de manera objetiva y científica estos fenómenos sociales, gracias a los cuales se puede lograr establecer un marco teórico bajo el cual se presentará el siguiente trabajo.

La Política de Defensa Nacional 2020, en su Capítulo II "Entorno para la Defensa de Chile" punto 4 "Conflictos y amenazas a nivel global", establece que "además de las amenazas tradicionales y los conflictos interestatales, la seguridad de los Estados se ve afectada por nuevas amenazas, preocupaciones y otros desafíos que poseen una naturaleza diversa, para lo cual se requiere una aproximación multisectorial"[3], donde las capacidades de la Defensa Nacional son un pilar fundamental para poder enfrentarlas.

En la descripción de las amenazas señaladas en la Política de Defensa, sobresale la "naturaleza híbrida" de las potenciales amenazas, las cuales han aumentado a nivel mundial en los últimos años. Estas corresponden a actividades hostiles de origen interno o externo que combinan métodos y capacidades convencionales y no convencionales, coordinadas y ejecutadas tanto por agentes estatales como grupos u organizaciones no estatales,

1 MORALES, S. (2017). El futuro de la naturaleza de los conflictos armados. [En línea] 23 de noviembre de 2017. Recuperado el 03 de septiembre de 2021 de file:///C:/Users/Irojas/Downloads/Dialnet-ElFuturoDeLaNaturalezaDeLosConflictosArmados-6361708%20(3).pdf p. 3.

2 Ministerio de Defensa Nacional. (2020). *Política de Defensa Nacional de Chile 2020.* Santiago, Chile: Ministerio de Defensa Nacional de Chile. p. 43.

3 Ibíd. p. 42.

manteniéndose siempre bajo el umbral de agresión que conlleva una respuesta militar por parte de los Estados afectados[4].

La Política de Defensa Nacional establece que estas actividades hostiles tienen el potencial de dañar a la población e infraestructura crítica, desestabilizar los procesos políticos democráticos o debilitar la capacidad de respuesta de un Estado frente a amenazas a su soberanía, integridad territorial o independencia política. Es por esta razón que también se establece la necesidad de contar con las capacidades estratégicas que permitan enfrentar, de manera disuasiva, o la capacidad de desarticular la combinación disruptiva de modos y medios de dichas potenciales amenazas híbridas.

Del mismo modo, se establece la necesidad de generar nuevas capacidades y medidas para enfrentar este tipo de amenazas, estableciéndose de manera general la necesidad de "incrementar la coordinación interagencial en materias como ciberseguridad, inteligencia y cooperación internacional. Lo anterior debe incluir la coordinación entre las instituciones de la Defensa, las policías, extranjería y aduanas"; se establece también la necesidad de "potenciar las capacidades de operaciones en ambientes multidominio, con especial énfasis en el dominio cognitivo o de la información", adicionalmente se debe considerar "la integración de fuerzas altamente entrenadas con capacidad de maniobra en el ambiente de la información y escenario de amenaza híbrida". Finalmente, señala la necesidad de potenciar las capacidades de "anticipación, elaboración de escenarios y doctrina, alistamiento operacional y respuesta, entrenamiento conjunto e interagencial para operar en un ambiente híbrido"[5].

Como podemos apreciar, lo establecido en la Política de Defensa Nacional (2020) y en el Libro de la Defensa Nacional de Chile (2017), se genera la necesidad de conocer las características y poder identificar estas "amenazas híbridas", que pueden afectar, ya sea directa o indirecta, al menos las áreas de misión de la "Soberanía e Integridad Territorial", la "Seguridad e Intereses Territoriales" y el "Desarrollo Nacional y la Acción del Estado".

Al leer la Política de Defensa Nacional, podemos inferir que no se establecen ni clasifican las potenciales amenazas que debe enfrentar la Defensa, para que así los organismos responsables puedan generar las capacidades estratégicas que permitan la desarticulación de la combinación disruptiva de los métodos y medios que empleen dichas potenciales amenazas.

Es por lo anterior que se procederá a realizar una clasificación de las principales amenazas híbridas que podrían afectar al Estado de Chile, para luego definir cuáles podrían ser los efectos en la Política de Defensa Nacional.

Los conflictos armados contemporáneos, que son el área de incumbencia específica de la "polemología"[6], han comenzado a sufrir una transformación hacia lo que se ha establecido como la necesidad de enfrentar nuevas amenazas o como se denominan hoy "amenazas híbridas" las que combinan características de al menos dos amenazas en un

4 Ibíd. p. 43.

5 Ibíd. p. 97.

6 Comprende "el estudio objetivo y científico de la guerra como fenómeno social susceptible de observación", de acuerdo a la definición de la Real Academia Española.

estado "puro", o de una amenaza en estado puro y otro fenómeno o situación de características diferentes. Esto hay que entenderlo de tal forma que las amenazas de un conflicto híbrido pasan a constituirse como un actor que plantea modos diferentes de combate, a los empleados de manera tradicional, y también como una amenaza que posee características que resultan de algún tipo de combinación entre al menos dos amenazas diferentes que se presentan de manera individual, o de al menos una amenaza y un fenómeno de otro tipo[7].

I. Aproximación al concepto de amenazas híbridas

Antes de comenzar a hablar de amenazas híbridas y establecer qué entenderemos por ellas, es necesario que comprendamos algunos conceptos asociados, como son la "guerra híbrida" y el "conflicto híbrido", ya que usualmente son empleados como sinónimos por aquellos que no conocen el significado real y las diferencias de estos conceptos, razón por la cual es importante hacer las aclaraciones respectivas para su correcto empleo.

Es así como entenderemos a la guerra híbrida como la "situación en la que un país o Estado recurre al uso abierto de las Fuerzas Armadas contra otro país, o contra un actor no estatal, además de usar otros medios (por ejemplo, económicos, políticos o diplomáticos)"[8].

Otra definición elaborada por el Dr. Frank Hoffman establece que la guerra híbrida combina la letalidad del conflicto estatal con el fervor fanático y prolongado de la guerra irregular. En este tipo de conflictos los adversarios, Estados, grupos patrocinados por el Estado o actores autofinanciados, explotan el acceso a las capacidades militares modernas, de la guerra regular, incluidos misiles y otros sistemas modernos, así como promover insurgencias prolongadas que emplean emboscadas, artefactos explosivos improvisados (IED abreviatura del inglés *improvised explosive device*) y asesinatos coercitivos, pertenecientes a elementos de la guerra irregular. Esto puede incluir Estados que combinan capacidades de alta tecnología como armas antisatélite con terrorismo y guerra cibernética dirigida contra otros objetivos como los financieros[9].

Como conflicto híbrido entenderemos a los fenómenos que poseen características propias, que comprenden una transformación de la violencia, la que es identificada en el contexto internacional a partir del año 2006; es así como se hace una diferencia de los conflictos asimétricos, ya que corresponden a una "situación en la cual las partes se abstienen del uso abierto de la fuerza (armada) y actúan combinando la intimidación militar (sin llegar a un ataque convencional) y a la explotación de vulnerabilidades económicas, políticas, tecnológicas y diplomáticas"[10]. En lo que fue la acción de Al Qaeda contra las Torres Gemelas, podemos apreciar el empleo de la "difusión mediática de las imágenes que constituye una estrategia capital. El hecho que hayan utilizado la televisión satelital para movilizar sus apoyos, forma

7 BARTOLOMÉ, M. (2019). Amenazas y conflictos híbridos: características distintivas, evolución en el tiempo y manifestaciones preponderantes. URVIO, *Revista Latinoamericana de Estudios de Seguridad* (25), 8-23. p. 9.

8 GALÁN, C. (2018). Amenazas Híbridas nuevas herramientas para viejas aspiraciones Fecha de consulta 25 de agosto 2021. Disponible en: https://www.realinstitutoelcano.org/documento-de-trabajo/amenazas-hibridas-nuevas-herramientas-para-viejas-aspiraciones/ p. 4.

9 HOFFMAN, F. (2009). Hybrid Warfare and Challenges. (Col David H. Gurney, Ed.) *Joint Force Quarteerly* (52), 34-39. Obtenido de: https://ndupress.ndu.edu/portals/68/Documents/jfq/jfq-52.pdf . p 39.

10 GALÁN. Loc. Cit.

parte de esa estrategia"[11]. En otras interpretaciones de los conflictos híbridos se señala que, "más allá de la violencia física, estos acontecimientos pueden expresarse en varios planos simultáneos, entre ellos el económico, legal, cibernético, comunicacional y mediático"[12].

En cuanto a las "amenazas híbridas" debemos iniciar por comprender lo que entenderemos por su concepto, donde "amenaza" se identifica como "una acción real o un hecho provocado, consciente o inconscientemente por un eventual adversario, que es percibida como una promesa de dañar intereses propios, porque a ese adversario se le supone, con cierto fundamento, la intención y la capacidad para hacerlo"[13]. Por otro lado, el concepto "híbrido" se entiende como "algo que es producto de elementos de distinta naturaleza"[14].

Ya entrando de lleno a lo que sería la definición de las "amenazas híbridas" podemos partir por establecer la visión de algunas autoridades de los Estados Unidos, como es el caso del Jefe de Estado Mayor del Ejército, quien escribía en el Army Magazine que las amenazas híbridas son: "combinaciones diversas y dinámicas de capacidades convencionales, irregulares, terroristas y criminales, las que harán difícil la utilización de enfoques singulares, siendo necesario soluciones híbridas e innovadoras que impliquen nuevas combinaciones de todos los elementos del poder nacional"[15].

También de los Estados Unidos, el Dr. Frank Hoffman ha señalado sobre las guerras híbridas y sus amenazas que los adversarios (Estados, grupos patrocinados por el Estado o actores autofinanciados) explotarán tanto las capacidades militares, con sus sistemas de armas modernos, así como el empleo de medios de insurgencias tales como las emboscadas, artefactos explosivos improvisados (IED) y asesinatos coercitivos y sin duda algunos no dejarán de emplear las capacidades que brinda la guerra cibernética, dirigida contra objetivos como los financieros u otros que le otorguen la posibilidad de lograr sus metas[16].

Por otro lado, la Unión Europea establece que:

> *"Las Amenazas Híbridas combinan actividades convencionales y no convencionales, militares y no militares que pueden ser utilizadas de manera coordinada por actores estatales o no estatales para lograr objetivos políticos específicos. Las campañas híbridas son multidimensionales y combinan medidas coercitivas y subversivas, utilizando herramientas y tácticas tanto convencionales como no convencionales. Están diseñadas para ser difíciles de detectar o atribuir. Estas amenazas apuntan a vulnerabilidades críticas y buscan crear confusión para dificultar la toma de decisiones rápidas y eficaces.*

11 GRAY, J. (2004). Al Qaeda y lo que significa ser moderno. Ed. Paidos. Recuperado el 07 de septiembre de 2021 de: https://issuu.com/vm2k14/docs/gray_john_-_al_qaeda_y_lo_que_signi . p. 109.

12 BARTOLOMÉ, M. Op. Cit. p. 11.

13 BANEGAS, A. (2017). ¿Existen estrategias para combatir las Amenazas Multidimensionales en la región? *Revista Política y Estrategia* (129), 89-120. p. 94.

14 De acuerdo a la definición de la Real Academia Española.

15 CASEY, G. (2008). America's Army In an Era of Persistent Conflict. Army Magazine, 58 (10), p. 24.

16 HOFFMAN. Op. Cit. p. 37..

> *Las Amenazas Híbridas pueden abarcar desde ataques cibernéticos a sistemas de información críticos, pasando por la interrupción de servicios críticos como el suministro de energía o los servicios financieros, hasta el debilitamiento de la confianza pública en las instituciones gubernamentales o la profundización de las divisiones sociales"*[17].

Finalmente, la Política de Defensa Nacional de Chile establece que las amenazas de naturaleza híbrida corresponden a:

> "*Actividades hostiles de origen interno o externo que combinan métodos y capacidades convencionales y no convencionales (campañas de desinformación, ciberataques, terrorismo, sabotaje, insurgencia, etc.), coordinadas o ejecutadas tanto por agentes estatales como otros grupos u organizaciones no estatales, manteniéndose, en general, bajo el umbral de agresión que conlleve una respuesta militar convencional por parte de los Estados afectados*"[18].

Como se ha podido apreciar en los conceptos de amenazas híbridas descritos, ellas pueden ser empleadas por parte de los Estados como por agentes no estatales y abarcan formas de enfrentamiento tanto violentas como no violentas, además dentro de sus objetivos estas pretenden no solo causar un daño directo a la población, o aprovechar las vulnerabilidades de ella, sino que también la posibilidad de desestabilizar la sociedad y crear grandes incertidumbres que dificulten la toma de decisiones por parte de los líderes de un Estado[19].

II. Amenazas híbridas

Ya hemos establecido qué se entiende por "amenazas híbridas" y las diferencias que existen con los conceptos de "guerra híbrida" y "conflicto híbrido"; ahora procederemos a describir algunas de las principales amenazas híbridas que podrían afectar a nuestro país.

1. *Campañas de desinformación o ataques de desinformación:* Se suelen definir como acciones con contenido falso difundido con la intención específica de engañar o manipular. No se trata de información errónea, se trata de la intención de impartir información falsa. La desinformación puede emplear muchos métodos: noticias de toda la vida, tuits o publicaciones de Facebook e Instagram; anuncios pagados en redes sociales e, incluso, grabaciones tendenciosamente editadas distribuidas en las redes sociales o mediante aplicaciones de mensajería. Según la Comisión Europea, "la desinformación o noticias falsas consisten en información demostrablemente falsa

17 Unión Europea. (2018). A Europe that protects: Countering hybrid threats. Recuperado el 13 de septiembre de 2021 de https://eeas.europa.eu/sites/default/files/hybrid_threats_en_final.pdf (Traducción del autor).

18 Ministerio de Defensa Nacional (2020). Op. Cit. p. 43.

19 INISEG. (2018). ¿Qué son y cómo nos afectan las Amenazas Híbridas? Instituto Internacional de Estudios en Seguridad Global. Recuperado el 09 de septiembre de 2021 de: https://www.iniseg.es/blog/seguridad/que-son-y-como-nos-afectan-las-amenazas-hibridas/

o incorrecta que es elaborada, presentada y difundida para obtener una ganancia económica, para engañar de manera maliciosa al público o para causar un daño"[20].

2. *Ciberguerra*: Corresponde a un "conflicto bélico en el que el ciberespacio y las tecnologías de la información son el escenario principal"[21]. Este tipo de conflictos se desarrolla en el ciberespacio, que corresponde al "dominio global y dinámico compuesto por infraestructuras de tecnologías de la información, las redes y los sistemas de información y telecomunicaciones"[22], normalmente es empleada para realizar ataques a lo que denomina infraestructura crítica "sistemas, máquinas, edificios o instalaciones relacionados con la prestación de servicios esenciales"[23]. Algunos ejemplos son las operaciones de los piratas informáticos pertenecientes a Estados como Rusia y China, quienes emplean armas cibernéticas para el logro de diferentes objetivos, actividades que se ven facilitados por las dificultades de determinar las responsabilidades y la ausencia de normas de comportamiento estatal en el ciberespacio[24].

3. *Crimen Organizado*: Se caracteriza por su naturaleza transnacional, opacidad, flexibilidad, capacidad de adaptación y de recuperación, así como por su movilidad. Desestabiliza los cimientos políticos y económicos de los Estados y, a su vez, estimula círculos viciosos de inseguridad, en la medida en que los integrantes de las redes criminales pueden colaborar con gobiernos corruptos, organizaciones paramilitares o grupos terroristas[25]. Algunos ejemplos corresponden a los grupos criminales armados y los carteles de la droga en México que recurren a la violencia en la lucha por el territorio y las ganancias económicas. La erosión de la seguridad, a su vez, tiene un impacto negativo en la economía del país[26].

4. *Corrupción*: Denominado también como estado mafioso y luego estado criminal comprende una posición en que la figura es el resultante de una penetración criminal a las estructuras estatales en un grado sin precedentes, corolario de largos procesos de criminalización, que reconocen diferentes estadios. Los funcionarios se enriquecen a sí mismos, y a sus familias y amistades, a través de la explotación de dinero, poder, influencia política y conexiones con el crimen organizado, que constituye la principal prioridad. Dicho de otra manera, las actividades ilegales no son realizadas solamente por profesionales de ese rubro, sino también por funcionarios públicos[27].

---

20 LISA Institute. (2019). Ataques de desinformación: qué son y cómo podemos evitarlos. Recuperado el 13 de septiembre de 2021 de: https://www.lisainstitute.com/blogs/blog/ataques-desinformacion-que-son-como-evitarlos

21 QUINTANA, Y. (2016). Ciberguerra. Editorial Los Libros de la Catarata, Madrid, España. p. 42.

22 Ibíd. p. 45.

23 Ibíd. p. 95.

24 PAWLAK, P. (2015). Understanding hybrid threats. Recuperado el 21 de septiembre de 2021 de: https://simulacion.hostking.cl/wp-content/uploads/2021/07/Parlamento-Europeo-Amenazas-Hibridas-Ingles.pdf p. 2.

25 Departamento de Seguridad Nacional. (2021). Crimen organizado. Recuperado el 14 de septiembre de 2021 de: https://www.dsn.gob.es/es/sistema-seguridad-nacional/qu%C3%A9-es-seguridad-nacional/%C3%A1mbitos-seguridad-nacional/crimen-organizado

26 PAWLAK. Op. Cit. p. 2

27 BARTOLOMÉ. Op. Cit. p. 18.

5. *Crisis financiera provocada*: Crisis financiera es aquella crisis económica que se origina por problemas relacionados con el sistema financiero o sistema monetario de un país. Cuando se produce dicho fenómeno el sistema financiero pierde valor y credibilidad. Dado que dicho sistema financiero guarda relación con la evolución de los negocios y la actividad económica, el desequilibrio produce perturbaciones que dan lugar a problemas de gran calado en los que los activos pierden su valor rápidamente. Todo ello con los consecuentes efectos que, *a posteriori*, deriva en la economía real. La crisis financiera está asociada a problemas relacionados con el sistema bancario, la deuda, los mercados de divisas, los mercados financieros, el pago de los países, etc[28].

6. *Epidemias y pandemias*: Se cataloga como epidemia a una enfermedad que se propaga rápida y activamente con lo que el número de casos aumenta significativamente, aunque se mantiene en un área geográfica concreta; por otro lado, para declarar el estado de pandemia deben cumplirse dos criterios: que la enfermedad afecte a más de un continente y que los casos de cada país ya no sean importados sino transmitidos comunitariamente[29].

7. *Flujos migratorios irregulares*: Comprenden un número de migrantes internacionales que llegan a un país (inmigrantes) o parten de un país (emigrantes) en el transcurso de un periodo de tiempo específico[30]. Para que se puedan considerar una amenaza estos flujos migratorios deben ser a gran escala, como ocurre en Europa o los Estados Unidos, los flujos migratorios que ocurren en otros países como Chile aún son muy pequeños para ser considerada una amenaza.

8. *Insurgencia*: Se denomina insurgencia al movimiento que un grupo de personas lleva a cabo en contra de una figura de poder o a favor o en contra de una causa en particular. Los movimientos de insurgencia pueden ser efectuados tanto por civiles, fuerzas militares como por grupos sindicales. La insurgencia conlleva en sí misma a la rebeldía, los manifestantes o insurgentes desean dejar claro su postura en contra de una autoridad o irregularidad y cuál será la posición en la cual se encontrarán según la situación. La desobediencia civil o el incumplimiento de algunas obligaciones suele ser el modo más sutil de realizar un acto de insurgencia. Sin embargo, existen casos en los cuales es inevitable el enfrentamiento armado entre los cuerpos de seguridad y los insurgentes.

9. *Narcotráfico*: Es el comercio ilegal de drogas tóxicas en grandes cantidades. El proceso se inicia con el cultivo de las sustancias, sigue con la producción y finaliza con la distribución y la venta, suele ser realizado por diversas organizaciones ilícitas las que se denominan carteles, los que se especializan en distintas partes de la cadena de producción y distribución. Los grupos más grandes dedicados al narcotráfico suelen tener presencia internacional y ostentan un gran poder. Sus integrantes cuentan

28 SEVILLA, A. (2012). Mercados financieros: Qué son, funciones y características. Recuperado el 21 de septiembre de 2021 de: https://economipedia.com/definiciones/mercados-financieros.html

29 Pontificia Universidad Católica de Chile. (2021). ¿Epidemia, pandemia o endemia? Recuperado el 23 de septiembre de 2021 de: https://observatorio.medicina.uc.cl/epidemia-pandemia-o-endemia/

30 O´REILLY, K. (2012). Toolkit on International Migration. Recuperado el 24 de septiembre de 2021 de: http://www.un.org/en/development/desa/population/migration/publications/others/docs/toolkit_DESA_June%202012.pdf p. 3.

con amplio tipo de armamentos y sus líderes manejan inmensas sumas de dinero. La condición de ilegal de las drogas provoca que estas adquieran un gran valor económico. Por otro lado, se sabe que las personas que sufren de adicción no conocen límites cuando sienten la necesidad de consumir. Combinando estos factores con la pobreza de muchos adictos, es fácil comprender que el narcotráfico sea un negocio tan lucrativo como riesgoso[31].

10. *Terrorismo*: Jean-Marie Balencie lo define como "Una secuencia de actos de violencia, debidamente planificada y altamente mediatizada, que toma deliberadamente como blanco a objetivos no militares a fin de crear un clima de miedo e inseguridad, impresionar a la población e influir en los políticos con la intención de modificar los procesos de decisión (ceder, negociar, pagar, reprimir) y satisfacer unos objetivos (políticos, económicos o criminales) previamente definidos"[32].

    Una de las formas de hibridización del terrorismo lo relaciona con la guerra contemporánea, dado que ambos fenómenos comparten un "cambio de escala" en términos de violencia, aplicándola contra masas civiles a partir de justificaciones vinculadas a la noción de "responsabilidad colectiva"[33]. Sobre ese punto, Brito Gonçalves y Reis alegan que, cada vez más, el terrorismo se aproxima en intensidad a una guerra, justificando acciones de Estados que en otras épocas hubieran sido inaceptables[34]. Algunos ejemplos corresponden a organizaciones como Boko Haram, Al-Qaeda en la Península Arábiga (AQAP) e ISIL / Da›esh que operan en los territorios de muchos países y emplean una variedad de herramientas económicas, militares y tecnológicas para lograr sus objetivos políticos.

11. *Piratería*: Esta expresión se refiere a actos de utilización que no han sido autorizados por el titular de derechos de autor o de derechos conexos, ni están contemplados en alguna excepción establecida expresamente por la ley respectiva. Con tales usos ilegítimos, se afecta la normal explotación de las producciones intelectuales que generan autores, artistas e industrias creativas.

    El término piratería es de uso habitual en materia de propiedad intelectual para referirse a las conductas ilícitas de reproducción (copia) y distribución de ejemplares de obras y producciones intelectuales[35].

---

31 PÉREZ P., Julian y GARDEY, Ana. Narcotráfico. [En línea] 2021 [Citado el: 03 de septiembre de 2021.] Disponible en: https://definicion.de/narcotrafico/

32 KHADER, Bichara (2010). El Mundo Árabe explicado a Europa. Historia, imaginario, cultura, política, economía, geopolítica. Barcelona: Icaria & IEMed., citado por RODRÍGUEZ Morales, Tania G. (2012) El terrorismo y nuevas formas de terrorismo, Espacios Públicos vol. 15, núm. 33, enero-abril, pp. 72-95. Recuperado el 27 de agosto de 2021 de: https://www.redalyc.org/pdf/676/67622579005.pdf

33 RUGGIERO, G. (2009). [Reseña sobre] CERLETTI, Alejandro. La enseñanza de la filosofía como problema filosófico, Buenos Aires, Libros del Zorzal, 2008, 94p. Revista de Filosofía y Teoría Política (40), 170-171. https://www.memoria.fahce.unlp.edu.ar/art_revistas/pr.3915/pr.3915.pdf

34 BARTOLOMÉ, M. Op. Cit. p. 11.

35 Instituto Nacional de Propiedad Intelectual. (2018). Observancia. Piratería y falsificación. Recuperado el 21 de septiembre de 2021 de https://www.inapi.cl/protege-tu-idea/pirateria-y-falsificacion

12. *Riesgos medioambientales*: Se denomina riesgo ambiental a la posibilidad de que por forma natural, por acción humana o la inacción, se produzca daño en el medio ambiente que afecte directamente a la población. Desde la perspectiva de las normas ISO 14001:2015, el riesgo se define como un efecto de incertidumbre, por lo que implica tanto efectos potenciales negativos como positivos, es decir amenazas y oportunidades[36].

13. *Sabotajes*: Daño o deterioro que se hace en instalaciones, productos, etc., como procedimiento de lucha contra organismos rectores, patronos, contra el Estado o contra las fuerzas de ocupación en conflictos sociales o políticos, o bien como método para beneficiar a una persona o grupo[37].

14. *Tráfico de Personas:* Se entenderá la captación, el transporte, el traslado, la acogida o la recepción de personas, recurriendo a la amenaza o al uso de la fuerza u otras formas de coacción, al rapto, al fraude, al engaño, al abuso de poder o de una situación de vulnerabilidad o a la concesión o recepción de pagos o beneficios para obtener el consentimiento de una persona que tenga autoridad sobre otra, con fines de explotación. Esa explotación incluirá, como mínimo, la explotación de la prostitución ajena u otras formas de explotación sexual, los trabajos o servicios forzados, la esclavitud o las prácticas análogas a la esclavitud, la servidumbre o la extracción de órganos[38].

15. *Tráfico ilícito de armas*: La importación, exportación, adquisición, venta, entrega, traslado o transferencia de armas de fuego, municiones, explosivos y otros materiales relacionados desde o a través del territorio de un Estado Parte al de otro Estado Parte si cualquier Estado Parte concernido no lo autoriza[39].

III. Clasificación de amenazas híbridas

Según lo establecido por Carlos Galán[40], las amenazas híbridas se pueden clasificar por su origen o por las herramientas empleadas por los agentes según los sectores que se emplean o se ven afectados por las amenazas híbridas. Adicionalmente, se presentará una subclasificación desarrollada por el autor.

1. Clasificación por su origen

- La localización de su autoría puede ser en el interior o en el exterior.

---

36 Esginnova Group. (2018). Riegos ambiental y análisis de los riesgos según la ISO 14.001 2015. Recuperado el 24 de septiembre de 2021 de https://www.nueva-iso-14001.com/2018/04/riesgo-ambiental-segun-la-iso-14001-2015/

37 De acuerdo a la definición de la Real Academia Española.

38 Organización de las Naciones Unidas. (2000). Protocolo contra el tráfico ilícito de migrantes por tierra, mar y aire, que complementa la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional. p. 2. Recuperado el 19 de septiembre de 2021 de: http://www.dpp.cl/resources/upload/files/documento/7a322932928aa3bb049d980b1540ae91.PDF

39 Organización de los Estados Americanos. (1997). Convención Interamericana contra la fabricación y el tráfico ilícito de armas de fuego, municiones, explosivos y otros materiales relacionados (A-63). p. 3. Recuperado el 13 de septiembre de 2021 de http://www.oas.org/es/sla/ddi/tratados_multilaterales_interamericanos_A-63_fabricacion_trafico_ilícito_armas_municiones_explosivos.asp

40 ALÁN. Op. Cit. pp. 9-11.

- La localización de su destino puede ser el Estado propio, terceros (aliados, no alineados o potencialmente enemigos) o el atacante.
- Los agentes que están detrás pueden ser Estados, empresas, corporaciones, delincuencia organizada, activistas y grupos de presión.

2. Clasificación por las herramientas empleadas por los agentes según los sectores

- *Militar*: Guerra no declarada, tropas no uniformadas, acciones encubiertas, utilización de organizaciones como la Contra centroamericana, los muyahidines en Afganistán o los Little Green men en Ucrania, los Lobos de la Noche en Crimea o la movilización de civiles.
- *Civil/Social*: Movimientos de protesta organizados por intereses extranjeros (Estados, corporaciones, troles...) y de contra protesta; creación de organizaciones locales de carácter económico (empresas), cultural o de opinión afines a los atacantes o patrocinadas por ellos; aprovechamiento de la influencia religiosa, lingüística o cultural para favorecer el "nihilismo social" o el "relativismo posmoderno", que alimentan campañas de desinformación.
- *Infraestructuras críticas*: Denegación de servicio y pérdida de integridad o confidencialidad de la información tratada.
- *Medios de comunicación*: propaganda (fácil y barata) mediante el uso de redes sociales originada en el exterior o incluso localmente; noticias falsas (*fake news*) con mensajes de texto, audio o video que provocan desinformación; operaciones psicológicas; uso de medios de comunicación afines o patrocinados (por ejemplo, RT y Sputnik en el caso de los intereses rusos y su difusión a través de partidos políticos, como el caso de M5S en Italia).
- *Económico*: Creación de empresas, centros de estudio y organizaciones culturales originarias de los países potencialmente atacantes o con intereses análogos; penetración en terceros países de los actores oligárquicos, con lazos en sectores políticos, económicos y en los medios de comunicación locales; recurso a la ayuda externa o sanciones económicas para presionar a un gobierno extranjero.
- *Político*: Diplomacia e inteligencia clásicas, poder blando, revelaciones y filtraciones, apoyo a simpatizantes en el exterior, chantajes y represalias.
- *Normativo*: Aprovechamiento de las lagunas legales.
- *Ciberespacio***:** Es empleado como medio para la ejecución de actividades de ciberespionaje, ciberdelincuencia o *hacktivismo*; uso de redes sociales (Twitter, Facebook, Instagram, etc.), incluidos grupos organizados de publicación de mensajes; revelaciones comprometedoras; desarrollos tecnológicos específicos.

3. Clasificación dentro del sector militar

Finalmente, a nuestro juicio también podemos hacer una subclasificación de las amenazas híbridas por los campos de acción de la Defensa, es así como podemos asociarlas a las capacidades que posee el Estado y la Defensa en particular, en las dimensiones físicas que

se emplean el Ejército (terrestre), la Armada (mar), la Fuerza Aérea (aire y el espacio ultra-terrestre) y el espectro electromagnético, teniendo en cuenta las capacidades polivalentes de las Fuerzas Armadas o propias del dominio de las armas en sus respectivos campos de acción de manera independiente o conjuntos.

Ilustración 1.- Amenazas y Desafíos para la Seguridad Nacional de España[41]

Las Fuerzas Armadas se deben encontrar preparadas para actuar en entornos con la presencia de amenazas asimétrica y amenazas de carácter híbrido, con una capacidad que de manera defensiva u ofensiva contrarreste las amenazas y, con ello, restringir el empleo o las acciones de grupos o Estados en contra de la población de nuestro país. "Para ello debe contar con un alto nivel de entrenamiento y alistamiento operacional, capaces de operar en

41 Gobierno de España. (2017). Estrategia de Seguridad Nacional 2017. Recuperado el 07 de septiembre de 2021 de https://www.defensa.gob.es/Galerias/defensadocs/Estrategia_Seguriad_Nacional_2017.pdf p. 79.

todo tiempo y escenarios, con gran apoyo de movilidad, inteligencia, vigilancia y reconocimiento, sistemas autónomos y no tripulados, integrados a nivel táctico, bajo una dirección y control en tiempo real desde niveles superiores"[42].

IV. Política de Defensa Nacional y efecto de las amenazas híbridas

En el desarrollo del presente capítulo se procederá a explicar la forma en que la Política de Defensa Nacional relaciona las amenazas y los conflictos con las capacidades estratégicas y las respectivas áreas de misión, para finalmente establecer cuáles son las influencias que poseen las amenazas híbridas sobre la Política de Defensa Nacional.

A. Política de Defensa Nacional

La Política de Defensa Nacional de Chile, desarrollada desde el año 1997 como parte de los Libros de Defensa o Estrategias de Seguridad y Defensa, de manera coordinada y coherente con la Política Exterior y la Política de Seguridad, entre otras, constituye una herramienta de conducción política para el jefe de Estado y un instrumento que contribuye a generar confianzas a nivel interno e internacional[43].

La Política de Defensa Nacional cumple con tres objetivos que corresponden con generar las directrices respecto a la Estrategia de la Defensa y su efecto en el desarrollo de las capacidades estratégicas y en la conducción política del sector y la Política Militar, establecer una declaración hacia la comunidad internacional respecto a la actitud y postura de Chile hacia la seguridad global y regional incluyendo la contribución de la Defensa Nacional y, finalmente, informar a la comunidad nacional respecto al rol de la Defensa en su contribución a la seguridad externa, interna y desarrollo del país[44].

Como se ha señalado de manera previa, la responsabilidad de la Seguridad y Defensa depende del jefe de Estado, comprendiendo tanto la seguridad externa como la seguridad interna, se entiende que la seguridad nacional es una condición alcanzable, la que requiere minimizar riesgos, disuadir y neutralizar amenazas. Es así como a través de la independencia política en la toma de decisiones, libres de coerción o influencia indebida, basada en el uso o amenaza del empleo de la fuerza u otros medios, pretende brindar la seguridad externa, evitando la acción de actores internacionales, junto a ello se encuentra mantener la "protección de la integridad territorial, la población y los intereses y recursos"[45].

Para que el jefe de Estado pueda dar cumplimiento a la tarea de mantener un entorno de seguridad adecuado para la población, cuenta con diferentes instrumentos de poder e influencia estatal, como la diplomacia, la información, el poder militar, la economía y el instrumento de poder interno[46], para ello se requiere que exista una adecuada coordinación entre las instituciones y organismos del Estado a fin de propender al bien común de la sociedad de manera integrada y cooperativa.

---

42 Ministerio de Defensa Nacional. (2020). Op. Cit. p. 60.

43 Ibíd. p. 7.

44 Ibíd. p. 9.

45 Ibíd. p. 11.

46 Ibíd. p. 12.

La Defensa es un bien público en un entorno cambiante lleno de riesgos, oportunidades y amenazas, que requiere de la participación y compromiso de las autoridades y de todos los ciudadanos, quienes en conjunto deben velar por la seguridad y defensa de los habitantes del país.

B. Conflictos y amenazas

Como se ha señalado con anterioridad, la Política de Defensa nos recuerda que los conflictos y amenazas globales pueden ser parte de las situaciones que deba enfrentar nuestro país, debido a nuestra dependencia económica mundial, y del libre comercio con grandes centros productores y consumidores a lo largo del mundo. Producto de ello, es que no solo nos podemos ver enfrentados a las amenazas tradicionales y los conflictos interestatales, sino que también vernos afectados por lo que se denomina las nuevas amenazas, preocupaciones y otros desafíos de naturaleza diversa[47].

Dentro de dichas amenazas se encuentran las de naturaleza híbrida, las que comprenden "actividades hostiles de origen interno o externo que combinan métodos y capacidades convencionales y no convencionales (campañas de desinformación, ciberataques, terrorismo, sabotaje, insurgencia, etc.), coordinadas o ejecutadas tanto por agentes estatales como otros grupos u organizaciones no estatales"[48].

Ilustración 2.- Conflictos y Amenazas a nivel Global (Elaboración propia).

Las amenazas híbridas poseen la capacidad de dañar tanto a la población como a la infraestructura crítica, desestabilizar la democracia y debilitar la capacidad de respuesta del Estado frente a su soberanía, integridad territorial y su independencia política[49].

C. Estrategia de la Defensa

La Estrategia de la Defensa se define a nivel político, ya que es el Presidente de la República quien lidera la tarea de garantizar el orden público en el interior y la seguridad externa del país, para ello es que cuenta con las capacidades estratégicas, normalmente

47 Ibíd. p. 42.

48 Ibíd. p. 43.

49 Ibíd.

representados por las Fuerzas Armadas, que son los medios para lograr los fines propuestos, los que se representan en los objetivos de la Defensa y sus respectivas Áreas de Misión asociadas, las que se encuadran en objetivos de seguridad externa y objetivos de seguridad interna y desarrollo[50].

Ilustración 3.- Estrategia de Defensa[51]

Ilustración 4.- Concepto estratégico por áreas de misión[52]

50 Ibíd. p. 51.

51 Ibíd.

52 Ibíd. 58.

Como se ha señalado de manera previa, de los objetivos de Defensa se desprenden las Áreas de Misión, las que corresponden a la "Defensa de la soberanía e integridad territorial", la "Cooperación Internacional y apoyo a la política exterior", la "Seguridad e intereses Territoriales", la "Emergencia nacional y protección civil" y finalmente la "Contribución al desarrollo nacional y la acción del Estado". Estas áreas de misión se encuentran establecidas con el propósito de poder determinar las capacidades estratégicas que la Defensa requiere para hacer frente a los fines de la defensa y así enfrentar los riesgos y amenazas.

La Política de Defensa establece así lo que se denomina el Concepto Estratégico de Empleo de la Defensa, el que se desarrolla para determinar la forma en que el Estado emplea su Defensa para el cumplimiento de las tareas establecidas en las diferentes Áreas de Misión. Se establece el Concepto Estratégico en Defensa de la Soberanía e Integridad Territorial donde el sector Defensa junto a la diplomacia, la economía y la información tienden a generar y mantener un entorno seguro[53].

Con el concepto Estratégico de Cooperación Internacional y Apoyo a la Política Exterior se busca generar beneficios para todos los países, establecer una situación de estabilidad y gobernanza en la región y el mundo para así disminuir la probabilidad de tener que usar la fuerza, tanto en contra del territorio nacional como en las áreas que se afecte a la población, el comercio y la economía[54]. El Concepto Estratégico en Seguridad e Intereses Territoriales, comprende aspectos como la soberanía efectiva sobre el territorio nacional, la seguridad e intereses marítimos, la seguridad en el ámbito aeroespacial nacional, los estados de excepción constitucional y votaciones populares y los intereses territoriales en la Antártica. El Concepto Estratégico en Emergencia Nacional y Protección Civil orientado a la necesidad de mantener un grado de preparación, planificación y definición de las posibles estructuras de mando y control que optimice las posibles respuestas ante situaciones derivadas de catástrofes naturales, antrópicas, emergencias sanitarias o cualquier otra que se presente, para con ello contribuir a mitigar los efectos de una emergencia en tiempos de paz[55]. Finalmente, el Concepto Estratégico en Contribución al Desarrollo Nacional y a la Acción del Estado, se orienta a la contribución y promoción del bien común, aportando al desarrollo del país, su conectividad, apoyo a zonas aisladas, preservación de tradiciones y valores patrios, fomentar la investigación, contribuir al desarrollo del plan espacial, entre muchos otros[56].

D. Capacidades Estratégicas

La Política de Defensa establece que la "Estrategia de la Defensa" es el resultado de la interacción entre fines y medios, mediante un concepto de empleo estratégico, el que se produce dentro de un marco delimitado por el entorno de seguridad, los posibles escenarios de empleo y los recursos disponibles, lo que implica necesariamente una decisión política para establecer los niveles de riesgo aceptables, entendiendo que no existe una solución perfecta ante la incerteza respecto a escenarios futuros de empleo de los medios[57].

53 Ibíd. 59.

54 Ibíd. 63.

55 Ibíd. 74.

56 Ibíd. 76.

57 Ibíd. p. 79.

La Política de Defensa ha clasificado las Capacidades Estratégicas en Áreas Generales de Capacidades Estratégicas, para de este modo agruparlas y generar un ordenamiento de las habilidades que deben contar las fuerzas para poder desempeñarse en el cumplimiento de sus objetivos en las diferentes áreas de misión. La Política de Defensa ha definido siete áreas generales de capacidades estratégicas de la Defensa, las que comprenden la Seguridad Operacional; Protección; Inteligencia, vigilancia y reconocimiento (ISR); Mando y Control Integrado; Movilidad y Proyección; Sostenibilidad y Despliegue Territorial.

Las Capacidades Estratégicas no son solo medios materiales que se emplean para el cumplimiento de los objetivos de la Defensa, sino que también integran factores como el entrenamiento, la doctrina, los recursos humanos, la organización, la información, el sostenimiento y la infraestructura, de forma tal que se complementan como un todo de manera sinérgica[58]. Es así como ellas deben ser evaluadas de manera permanente, para asegurarse que son capaces de enfrentar los desafíos y amenazas del entorno estratégico, que se torna muy cambiante.

Ilustración 5.- Capacidades Estratégicas[59]

58 Ibíd. p. 88.

59 Ibíd. p. 80.

Las amenazas híbridas y los conflictos híbridos también son parte del entorno que debe enfrentar la Defensa, por lo que bajo la lógica de planificación de la Defensa, hace necesario que se cuenten con las capacidades estratégicas para poder hacerles frente. Es importante señalar que las amenazas de tipo híbrido no se pueden enfrentar con el enfoque tradicional de la Defensa debido a sus características desarticuladoras y disruptivas.

E. Efecto de las amenazas híbridas

Como hemos podido apreciar a través del desarrollo de los puntos previos, la Política de Defensa es un documento que establece las orientaciones y directrices respecto a la Estrategia de la Defensa que debe seguir el país y su efecto en el desarrollo de capacidades estratégicas, tanto en la conducción política del sector como en la política militar. Por ello es que, al querer hacer frente a los conflictos híbridos y las amenazas híbridas, se deben adoptar estrategias relacionadas con una nueva política de seguridad empleando los medios y capacidades de la defensa de una forma diferente a la tradicional. Cabe hacer presente que esto no implica que se debe olvidar el conflicto tradicional para enfrentar estas nuevas amenazas, sino que simplemente la defensa debe incrementar sus capacidades e incorporar nuevas metodologías para poder hacerles frente, ya que además de las amenazas tradicionales hoy se encuentran presentes las amenazas híbridas.

Se debe considerar el desarrollo de nuevas capacidades estratégicas (doctrina, entrenamiento, medios para combatirla, infraestructura, recursos humanos, sostenimiento), para poder enfrentar este nuevo tipo de amenazas, donde la coordinación de los diferentes actores estatales en materias de ciberseguridad, inteligencia, cooperación internacional y otros juegan un papel fundamental.

La necesidad de explotar las capacidades del Estado como un todo que enfrente, inclusive con el apoyo de la ciudadanía, las nuevas amenazas o amenazas híbridas se hace fundamental, ya que no es solo el Estado quien deberá trabajar para el logro del bien común en post de brindar seguridad a su población, sino que los ciudadanos deberán ser un actor preponderante en las acciones que, de manera coordinada, se deberán elaborar para brindar seguridad a todos sus miembros.

Posterior al 11 de Septiembre y la caída de las Torres Gemelas, la guerra convencional ya no ha estado tan presente, han surgido nuevas interrogantes como son:

- ¿Quién es el enemigo?
- ¿Dónde está el enemigo?
- ¿Qué está haciendo o intentando hacer el enemigo?

Los escenarios donde se desarrollan los conflictos y donde se presentan las amenazas híbridas son diferentes a los tradicionales, estas nuevas amenazas requieren respuestas integrales, coordinadas y cooperativas, con una mejor conciencia de la situación para contrarrestar y responder a ellas.

La administración Política y de Defensa deberá generar nuevas estrategias relacionadas con las implicaciones que para la seguridad, las Fuerzas Armadas y la Defensa en general tendrán los conflictos híbridos. Su objetivo deberá ser el establecer la esencia y la naturaleza

de las amenazas híbrida, así como la lógica y el patrón de las estrategias híbridas, con el fin de desarrollar un método analítico sólido que sea la base para la evaluación de las situaciones de conflictos híbridos actuales y futuros, determinando sus implicaciones prácticas.

Las acciones deben tender a contribuir a mejorar la comprensión y los juicios comunes y completos de los miembros del Estado, como condición previa para lograr una mejor conciencia de la situación, así como para una acción que permita de manera conjunta e integrada contrarrestar y responder a las amenazas híbridas.

V. Conclusiones

El conflicto ha sido parte de la historia de la humanidad y como parte de esta historia su evolución en el tiempo ha implicado que ella vaya evolucionando. La tecnología ha sido parte importante de esa evolución; sin embargo, no ha sido solo eso, sino la forma de enfrentar el conflicto por los hombres lo que ha generado gran parte de esos cambios.

En la medida que nuestro país ha visto esa evolución va generando las directrices para sus diferentes organismos de manera de poder brindar la seguridad que pretende para su población, junto con las condiciones necesarias para que éste progrese. Es así como la Política de Defensa Nacional se ha actualizado hasta su última versión del año 2020, y dentro de estas actualizaciones se ha incorporado el concepto de amenazas híbridas lo que sin duda generará ciertos cambios en la forma de enfrentar el conflicto.

Como hemos podido conocer a través de lo expuesto de manera previa, a través de los diversos autores y las normativas que se han citado, podemos señalar que las amenazas híbridas son distintas a la guerra híbrida y los conflictos híbridos. Las amenazas híbridas corresponden a fenómenos que comprende la interacción de elementos de distinta naturaleza (convencionales y no convencionales) que poseen la capacidad de ejecutar una acción hostil coordinada tanto por agentes estatales o grupos y asociaciones no estatales, los que manteniendo un umbral de agresión baja evitan la acción militar convencional, algunas de estas corresponden a campañas de desinformación, ciberataques, terrorismo, sabotaje, insurgencia, entre otras.

Se ha presentado una clasificación de las amenazas, según lo que ha establecido la Unión Europea, la que ha manifestado una real preocupación por las amenazas y conflictos híbridos. Esta clasificación se basa en dos conceptos básicos: la clasificación que proviene por el origen de las amenazas y, en segundo lugar, por las herramientas que se emplean por los agentes según el sector en el que se emplean o se ven afectados.

Se propuso una subclasificación dentro del ámbito militar, la que considera los campos de acción de la Defensa, es así como se propone considerar las dimensiones físicas que se emplean por el Ejército (terrestre), la Armada (mar), la Fuerza Aérea (aire y el espacio ultraterrestre) y el espectro electromagnético, donde se consideran las capacidades polivalentes de las Fuerzas Armadas o las propias del dominio de las armas en sus respectivos campos de acción.

Se ha descrito la manera en la que la Política de Defensa Nacional de nuestro país ha evolucionado, con el propósito de generar las directrices respecto de lo que será la Estrate-

gia de Defensa del país y el desarrollo de las Capacidades Estratégicas y la conducción de la Política de Defensa y Militar.

En la Política de Defensa se establece la relación que tienen los conflictos y las amenazas, la Estrategia de Defensa y las Capacidades Estratégicas que se requieren para poder enfrentar a las amenazas a través de lo que se ha denominado las Áreas Generales de Capacidades Estratégicas y Áreas de Misión.

Finalmente hemos visto, de manera general, cuáles serán las influencias que tienen las amenazas híbridas sobre la Política de Defensa donde se ha señalado que se deberán adoptar estrategias tendientes a enfrentarlas que tienen un tratamiento diferente al tradicional, sin dejar de lado las amenazas tradicionales. Es así como se debe considerar el desarrollo de las capacidades estratégicas (doctrina, entrenamiento, medios para combatirla, infraestructura, recursos humanos, sostenimiento), para poder enfrentar este tipo de amenazas, donde la coordinación de los diferentes actores estatales en materias de ciberseguridad, inteligencia, cooperación internacional y otros, juegan un papel fundamental.

REFERENCIAS BIBLIOGRÁFICAS

BANEGAS Alfaro, Aracely: "¿Existen estrategias para combatir las Amenazas Multidimensionales en la región? Revista Política y Estrategia Nº 129, 2017 : 89–120. Disponible en: https://doi.org/10.26797/rpye.v0i129.72

BARTOLOMÉ, Mariano. Amenazas y conflictos híbridos: características distintivas, evolución en el tiempo y manifestaciones preponderantes. [En línea] *URVIO, Revista* Latinoamericana de Estudios de Seguridad, Quito (25) :8-23, diciembre 2019. Disponible en: http://revistas.flacsoandes.edu.ec/index.php/URVIO

CASEY, George. America's Army In an Era of Persistent Conflict. Army Magazine, Vol. 58: 19-22, octubre 2008.

COMITÉ INTERNACIONAL DE LA CRUZ ROJA. Documento de opinión. [En línea] Cuál es la definición de "conflicto armado" según el derecho internacional humanitario?, marzo 2008. p. 6. [Fecha de Consulta: 27 de 08 de 2021]. Disponible en: https://www.icrc.org/es/doc/assets/files/other/opinion-paper-armed-conflict- es.pdf

DEPARTMENT OF DEFENSE USA. [En línea] Home Land Security Digital Library. diciembre 2008. [Fecha de Consulta: 08 de septiembre de 2021]. Disponible en: https://www.hsdl.org/?view&did =233338

DEPARTAMENTO DE SEGURIDAD NACIONAL**.** Crimen Organizado. [En línea] 2021. [Citado el: 14 de 09 de 2021.] https://www.dsn.gob.es/es/sistema-seguridad-nacional/qué-es-seguridad-nacional/ámbitos-seguridad-nacional/crimen-organizado .

DEPARTAMENTO DE SEGURIDAD NACIONAL DE ESPAÑA. 2021. [Fecha de Consulta: el 25 de AGO de 2021]. Disponible en: https://www.dsn.gob.es/es/sistema-seguridad-nacional/qué-es-seguridad-nacional/ámbitos-seguridad-nacional/crimen- organizado

Esginnova Group**.** (2018). Riegos ambiental y análisis de los riesgos según la ISO 14.001 2015. Recuperado el 24 de septiembre de 2021, de: https://www.nueva-iso-14001.com/2018/04/riesgo-ambiental-segun-la-iso-14001-2015/

ESTADO MAYOR, Departamento del Ejército, Comando de Operaciones Especiales de los Estados Unidos. La Guerra no Convencional. [En línea] [Fecha de Consulta: 27 de 08 de 2021]. Disponible en: https://forocontralaguerra.files.wordpress.com/2016/01/circular_tc1801-guerra-no-convencional-manula-usa.pdf, noviembre 2010. 111p.

GALÁN, CARLOS. Amenazas híbridas, nuevas herramientas para viejas aspiraciones. [En línea] 13 de DIC de 2018. [Citado el: 25 de 08 de 2021]. Disponible en: http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/dt20-2018-galan-amenazas-hibridas-nuevas-herramientas-para-viejas-aspiraciones

GOBIERNO DE ESPAÑA**.** 2017. Estrategia de Seguridad Nacional 2017**.** [En línea] Recuperado el 07 de septiembre de 2021. Disponible en: https://www.defensa.gob.es/Galerias/defensadocs/Estrategia_Seguriad_Nacional_2017.pdf. 785170411

GRAUTOFF, M. (12 de JUN de 2007). www.redalyc.org. Revista de Relaciones Internacionales, Estrategia y Seguridad, 2(1), 131 - 144. Recuperado el 25 de 08 de 2021. Disponible en: https://www.redalyc.org/pdf/927/92720107.pdf

GRAY, Jhon**.** Al Qaeda y lo que significa ser moderno. Ed. Paidós. [En línea] 2004. [Recuperado el 07 de septiembre de 2021] Disponible en: https://issuu.com/vm2k14/docs/gray_john_-_al_qaeda_y_lo_que_signi .

HOFFMAN, FRANK. 2009. Hybrid Warfare and Challenges [ed.] USMC (Ret.) Col David H. Gurney. 52, 1 quarter de 2009, Joint Force Quarteerly, pp. 34-39.

INISEG**.** ¿Qué son y cómo nos afectan las Amenazas Híbridas? Instituto Internacional de Estudios en Seguridad Global. [En línea] 06 de agosto de 2018. [Recuperado el 09 de 09 de 2021.] Disponible en https://www.iniseg.es/blog/seguridad/que-son-y-como-nos-afectan-las-amenazas-hibridas/

INSTITUTO NACIONAL DE PROPIEDAD INTELECTUAL. Observancia**.** Piratería y Falcificación. [En línea] 2018. [Citado el: 21 de septiembre de 2021.] Disponible en: https://www.inapi.cl/protege-tu-idea/pirateria-y-falsificacion

KHADER, Bichara (2010). *El Mundo Árabe explicado a Europa. Historia, imaginario, cultura, política, economía, geopolítica.* Barcelona: Icaria & IEMed., citado por RODRÍGUEZ Morales, Tania G. (2012) El terrorismo y nuevas formas de terrorismo, Espacios Públicos vol. 15, núm. 33, enero-abril, pp. 72-95. Recuperado el 27 de agosto de 2021 de: https://www.redalyc.org/pdf/676/67622579005.pdf

LISA INSTITUTE**.** Ataques, desinformacion que son como evitarlos. [En línea] 27 de febrero de 2019. [Recuperado el 13 de septiembre de 2021.] Disponible en: https://www.lisainstitute.com/blogs/blog/ataques-desinformacion-que-son-como-evitarlos

MILOSEVICH-JUARISTI, M. La Guerra no Lineal. [30 de enero de 2015.] *www.realinstitutoelcano.org.* (R. I. Elcano, Ed.) Recuperado el 27 de agosto de 2021, de Disponible en: http://www.realinstitutoelcano.org/wps/wcm/connect/97391e00471fcf929132bb12dd3b68de/Comentario-MilosevichJuaristi-la-guerra-no-lineal-rusa.pdf?MOD=AJPERES &CACHEID=97391e00471fcf929132bb12dd3b68de

MINISTERIO DE DEFENSA NACIONAL. Política de Defensa Nacional de Chile 2020*.* Santiago: Ministerio de Defensa Nacional de Chile, 2020. p. 108.

MINISTERIO DE DEFENSA NACIONAL, 2017. Libro de la Defensa Nacional de Chile*.* Santiago: Ministerio de Defensa Nacional, 2017. p. 319.

MORALES, S. Conflictos Armados. [En línea] 23 de noviembre de 2017. Recuperado el 03 de SEP de 2021, de Disponible en: http://www.ieee.es/Galerias/fichero/docs_marco/2017/DIEEEM17-2017_Futuro_ConflictosArmados_SamuelMorales.pdf

ORGANIZACIÓN DE LAS NACIONES UNIDAS. (2000). Protocolo contra el tráfico ilícito de migrantes por tierra, mar y aire, que complementa la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional. p. 2. Recuperado el 19 de

septiembre de 2021. Disponible en: http://www.dpp.cl/resources/upload/files/documento/7a322932928aa3bb049d980b1540ae91.PDF

ORGANIZACIÓN DE LOS ESTADOS AMERICANOS. (1997). Convención Interamericana contra la fabricación y el tráfico ilícito de armas de fuego, municiones, explosivos y otros materiales relacionados (A-63). p. 3. Recuperado el 13 de septiembre de 2021 de http://www.oas.org/es/sla/ddi/tratados_multilaterales_interamericanos_A-63_fabricacion_trafico_ilicito_armas_municiones_explosivos.asp

ORGANIZACIÓN DE LOS ESTADOS AMERICANOS. Derecho Internacional Humanitario. (D. d. Internacional, Editor) Recuperado el 25 de 08 de 2021. Disponible en: http://www.oas.org/es/sla/ddi/derecho_internacional_humanitario.asp

ORGANIZACIÓN INTERNACIONAL PARA LA MIGRACIÓN. Migración. [En línea] Recuperado el 23 de septiembre de 2021, Disponible en: https://www.iom.int/es/sobre-la-migracion

O´REILLY, KAREN. Toolkit on International Migration. [En línea] 2012. [Recuperado el: 24 de 09 de 2021.] Disponible en: http://www.un.org/en/development/desa/population/migration/publications/others/docs/toolkit_DESA_June%202012.pdf

PAWLAK, PATRYK. Amenazas Hibridas. [En línea] junio de 2015. [Citado el: 21 de 09 de 2021.] Disponible en: https://simulacion.hostking.cl/wp-content/uploads/2021/07/Parlamento-Europeo-Amenazas-Hibridas-Ingles.pdf

PASCUAL, T. (SEP de 2020). Manual de Derecho Internacional de los Derechos Humanos para la Defensa Nacional Pública. Producción y edición Defensoría Nacional. Defensoría Nacional Pública. Recuperado el 27 de 08 de 2021, de https://biblio.dpp.cl/datafiles/16151-2.pdf

PÉREZ P., Julian y GARDEY, Ana. Narcotráfico**.** [En línea] 2021 [Citado el: 03 de SEP de 2021.] Disponible en: https://definicion.de/narcotrafico/

PONTIFICIA UNIVERSIDAD CATÓLICA DE CHILE. **¿Epidemia, pendemia o endemia?** [En línea] 2021. [Recuperado: 23 de septiembre de 2021.] Disponible en: https://observatorio.medicina.uc.cl/epidemia-pandemia-o-endemia/

QUINTANA, YOLANDA. *Ciberguerra.* Editorial Los Libros de la Catarata, Madrid, España, 2016.

RUGGIERO, G. (2009). [Reseña sobre] CERLETTI, Alejandro. La enseñanza de la filosofía como problema filosófico, Buenos Aires, Libros del Zorzal, 2008, 94p. [En línea] Revista de Filosofía y Teoría Política, 40, 170-171. Disponible en: http://www.fuentesmemoria.fahce.unlp.edu.ar/art_revistas/pr.3915/p r.3915.pdf

SCHNAUFER, T. Redefifining Hybrid Warfare: Russia's Non-linear War against the West. Journal of Strategic Security. [En línea] 10 (1), 17-31. Recuperado el 02 de septiembre de 2021. Disponible en: https://digitalcommons.usf.edu/cgi/viewcontent.cgi?article=1538&context=jss

SEVILLA, A. Mercados Financieros**:** Qué son, funciones y características. [En línea]. Recuperado el 21 de 09 de 2021. Disponible en: https://economipedia.com/definiciones/mercados-financieros.html

UNIÓN EUROPEA. A Europe that protects: Countering hybrid threats. [En línea]. Junio 2018. Recuperado el 13 de septiembre de 2021. Disponible en: https://eeas.europa.eu/sites/ default/ files/ hybrid_threats_en_final.pdf


ACADEMIA NACIONAL DE ESTUDIOS POLITICOS Y ESTRATEGICOS
CHILE

ESTUDIOS

DESCODIFICANDO LA INFRAESTRUCTURA CRÍTICA: CASO NACIONAL*∞

FULVIO QUEIROLO PELLERANO•

RESUMEN

Diversos incidentes, de carácter antrópico o natural, han afectado estructuras públicas y privadas, sean materiales o intangibles, provocando estragos en el buen desempeño funcional de servicios fundamentales que requiere un país, sociedad o colectivo. En este ámbito, numerosas administraciones estatales, organismos internacionales y organizaciones multilaterales han avanzado en identificar cuáles serían aquellos servicios y estructuras administrativas, cuya alteración o ruptura, podrían ver socavada su principal cometido. Dicho entorno se concibe como infraestructura crítica. Así las cosas, es posible observar que pese a todos los avances para otorgar una adecuada conceptualización, así como establecer niveles de responsabilidad en su protección, también es factible evidenciar que, para el caso nacional, la normativa no ha madurado adecuadamente. Por lo tanto, es esencial una definición rápida que contenga una descripción clara, así como una estrategia para proteger la infraestructura crítica nacional.

Palabras clave: *Infraestructura crítica; riesgo; amenaza; estrategia nacional.*

DECODING CRITICAL INFRASTRUCTURE: NATIONAL CASE

ABSTRACT

Various incidents, of an anthropogenic or natural nature, have affected public and private structures, whether material or intangible, wreaking havoc on the good functional performance of fundamental services required by a country, society or group. In this area, numerous state administrations, international and multilateral organizations have made progress in identifying those services and administrative structures whose alteration or rupture could see their main mission undermined.

---

* El escrito es resultado del trabajo de investigación elaborado durante la ejecución del programa de Seguridad Internacional, que desarrolla la Universidad Nacional de Educación a Distancia (UNED), conducente al grado académico de doctor.

• Magíster en Ciencia Política, Seguridad y Defensa (ANEPE). Doctorando en Seguridad Internacional (UNED, programa internacional, IUGGM, España). Investigador asociado Universidad UBO. Encargado de Estudios Estratégicos en Academia Nacional de Estudios Políticos y Estratégicos. Chile. fqueirolo@anepe.cl - fqueirolo3@alumno.uned.es ORCID: https://orcid.org/0000-0001-6837-0962

∞ Fecha de recepción: 030624 - Fecha de aceptación: 260624.

This environment is conceived as critical infrastructure. Thus, it is possible to observe that despite all the advances to provide an adequate conceptualization, as well as establish levels of responsibility in its protection, it is also possible to show that, in the national case, the regulations have not matured adequately. Therefore, a prompt definition containing a clear description as well as a strategy to protect national critical infrastructure is essential.

Key words: *Critical infrastructure; risk; threat; national strategy.*

DECODIFICANDO INFRAESTRUTURA CRÍTICA: CASO NACIONAL

RESUMO

Diversos incidentes, de natureza antropogénica ou natural, afectaram estruturas públicas e privadas, *sejam materiais ou imateriais, causando estragos no bom desempenho funcional de serviços fundamentais requeridos por um país, sociedade ou grupo. Nesta área, numerosas administrações estatais, organizações internacionais e organizações multilaterais têm feito progressos na identificação dos serviços e estruturas administrativas cuja alteração ou ruptura poderia ver prejudicada a sua missão principal. Este ambiente é concebido como infraestrutura crítica. Assim, é possível observar que apesar de todos os avanços para fornecer uma conceituação adequada, bem como estabelecer níveis de responsabilidade na sua proteção, também é possível mostrar que, no caso nacional, a regulamentação não amadureceu adequadamente. Portanto, é essencial uma definição* rápida que *contenha uma descrição clara, bem como uma estratégia para proteger as infra-estruturas críticas nacionais.*

Palavras-chave: *Infraestrutura crítica; risco; ameaça; estratégia nacional.*

Introducción

Evidencias sobre una creciente manifestación de elementos perturbadores, cuya consecuencia ha sido infringir daños en estructuras físicas e intangibles, principalmente sobre servicios públicos, proveedores privados, así como en organizaciones e instalaciones gubernamentales, exige una debida consideración. ¿Cuáles serían estos elementos perturbadores y qué estructuras se han visto comprometidas? ¿Quiénes debiesen asumir la responsabilidad de protegerlas? Son preguntas que requieren de una robusta respuesta por parte del Estado y previsión por parte de privados. En palabras simples, es necesario separar la nata de la leche para obtener un buen producto.

La aproximación más afín sobre esta discusión es la proporcionada por la Organización para la Cooperación y el Desarrollo (OCDE), al señalar:

"Los riesgos críticos pueden derivarse de fenómenos naturales, pandemias, accidentes industriales o tecnológicos graves y actos malintencionados que provoquen daños de importancia nacional. Sus consecuencias pueden provocar trastornos en sectores de la infraestructura vitales para las actividades económicas, degradar bienes ambientales clave, causar un efecto negativo en las finanzas públicas y erosionar la confianza pública en el gobierno. Ante un complejo escenario de cambios demográficos, adelantos tecnológicos, globalización y cambio climático, los riesgos críticos pueden desarrollarse con rapidez y por vías imprevistas, permitiendo que los impactos transfronterizos se dispersen en diferentes comunidades, sectores económicos y fronteras nacionales"[1].

El criterio, con visión económica, recomendado por la OCDE para definir una infraestructura crítica (IC) contempla "… *los sistemas, activos, instalaciones y redes que prestan servicios esenciales para el funcionamiento de la economía y para la seguridad, la protección y el bienestar de la población"*[2]. Si bien se orienta hacia el desarrollo y bienestar, no delimita si dichos servicios son solo provistas por el Estado y/o bien con participación de proveedores privados. Del mismo modo, deja abierta a la interpretación sobre la extensión de cuáles serían aquellos elementos perturbadores o amenazas que podrían afectar a la IC de servicios esenciales.

En el entorno descrito resulta fundamental contar con una eficaz y oportuna inteligencia que permita identificar cuáles serían aquellos riesgos y amenazas a la que se enfrenta un servicio, organización o instalación crítica. El diseño de estrategias nacionales, regionales y locales constituye el eslabón principal en la cadena de formación de una sociedad preparada y resiliente.

La condición actual de la normativa nacional presenta aspectos subjetivos y falta de especificidad en los niveles de gestión gubernamental. Así las cosas, se pone en riesgo la aplicabilidad de los criterios establecidos, un ambiente que, más temprano que tarde, se expone a juicios de interpretación y confusión de los actores del régimen establecido. Esta hipótesis se sustenta en lo indicado por el numeral 21 de la Ley Nº 21.542, que modificó la Carta Fundamental, al disponer que las fuerzas armadas asuman responsabilidades en la protección de la IC, prescribiendo:

> *"Disponer, mediante decreto supremo fundado, suscrito por los Ministros del Interior y Seguridad Pública y de Defensa Nacional, que las Fuerzas Armadas se hagan cargo de la protección de la infraestructura crítica del país cuando exista peligro grave o inminente a su respecto, determinando aquella que debe ser protegida"*[3].

En consideración a la relevancia de la temática el presente ensayo pretende llevar a cabo un juicio crítico sobre la capacidad de aplicación de la ordenanza nacional destinada al

---

1 OECD. "Recomendación del Consejo sobre la Gobernanza de Riesgos Críticos". 6 de mayo de 2014. En: https://www.oecd.org/gov/risk/Critical-Risks-Recommendation-Spanish.pdf

2 OCDE. "*Recomendación del Consejo sobre la gobernanza de infraestructuras*", OECD/LEGAL/0460, p. 6, 2020. En: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0460

3 BCN. Ley Nº 21.542. "Modifica *la carta fundamental con el objeto de permitir la protección de infraestructura crítica por parte de las fuerzas armadas, en caso de peligro grave o* inminente". 3 febrero, 2023. En: https://www.bcn.cl/leychile/navegar?idNorma=1188583

resguardo de la IC. Su objetivo se centrará en identificar factores que requieren ajustes y así alcanzar una efectiva sincronización de los agentes involucrados para la protección de la IC.

Para dilucidar la hipótesis planteada, se utilizará el método de cotejo de la normativa nacional comparándola con el régimen convenido a partir de lo establecido por la Unión Europea (UE), a través del Consejo Europeo y, posteriormente, sistematizado por la OCDE. La técnica escogida permitirá revelar aspectos sensibles que contribuirán a clarificar el planteamiento, así como aportar elementos para la discusión nacional.

La codificación de la infraestructura crítica (IC)

Literatura internacional respecto de la temática es nutrida, sin embargo, con el fin de acotar el examen propuesto, se seleccionarán tres perspectivas que permitan llevar a cabo una decodificación del concepto. La necesidad de decodificar surge de la perspectiva del estudio propuesta buscando descifrar conceptos. De esta manera, se analizará la ruta que han trazado organizaciones y entidades que presentan una evolución sostenida en el tratamiento de la IC., y a partir de dicha base sustentar el alcance de la conceptualización a nivel nacional.

- **Del proceso del Consejo Europeo y la Comisión**

- A partir de los atentados terroristas perpetrados en Madrid (11/03/2004) y Londres (7 y 21/07/2005), respectivamente, el Consejo Europeo mandató a la Comisión Europea para llevar a cabo un trabajo, cuyo resultado fue el diseño de una estrategia para la protección de la IC[4].

- El Consejo de Ministros, desde un principio, asumió que las IC podían ser dañadas por "*acciones terroristas deliberadas, catástrofes naturales, accidentes o actos de piratería informática, actividades delictivas o comportamientos malintencionados*".

- Con todo, el objetivo de la Comisión estuvo focalizado en brindar protección de sus activos de acciones de terrorismo. El resultado fue la elaboración un Libro Verde[5] cuyos lineamientos se orientaban sobre el resguardo de la infraestructura de la Comunidad Europea. En esta ruta se asumió de forma consensuada la siguiente definición de IC.:

> *"… aquellos recursos físicos, servicios e instalaciones, redes y activos de infraestructura de tecnología de la información que, si se interrumpieran o destruyeran, tendrían un impacto grave en la salud, la seguridad o el bienestar económico de los ciudadanos o el funcionamiento eficaz de los gobiernos"*[6].

4 COMISIÓN EUROPEA. "*Critical Infrastructure Protection in the fight against terrorism*". Brussels, 20.10.2004 COM (2004) 702 final, de 20 de octubre de 2004. En: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0702:FIN:EN:PDF

5 COMISIÓN DE LAS COMUNIDADES EUROPEAS. Libro Verde. "*Sobre un programa europeo para la protección de infraestructuras críticas".* Bruselas. 17.11.2005. Anexo 1, p. 22. En: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0576:FIN:ES:PDF

6 UE. Directiva 2008/114/CE del Consejo de la UE. "*Sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección"*. 8 diciembre 2008. En: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32008L0114

- Sin embargo, la discusión continuó avanzando conforme a nuevos entornos de riesgos y amenazas, que se ciernen sobre la Comunidad Europea, estableciendo e identificando una infraestructura crítica europea (ICE) para esta Comunidad como:

> *"… el elemento, sistema o parte de este situado en los Estados miembros que es esencial para el mantenimiento de funciones sociales vitales, la salud, la integridad física, la seguridad, y el bienestar social y económico de la población y cuya perturbación o destrucción afectaría gravemente a un Estado miembro al no poder mantener esas funciones"*[7].

- Tras la agresión rusa hacia Ucrania, así como la interrupción de servicios esenciales en áreas de Europa anexado a la crisis energética ocasionada por el corte de tuberías del gasoducto *Nord Stream,* reactivó el debate europeo para la actualización de una nueva agenda de seguridad. En esta oportunidad, el objetivo fue incorporar nuevos riesgos en ICE, articulando el advenimiento de amenazas híbridas. El parámetro de recomendaciones del Consejo se sitúa en:

> *"… la sociedad depende en gran medida de infraestructuras tanto físicas como digitales y la interrupción de los servicios esenciales, ya sea por ataques físicos convencionales o por ciberataques, o por una combinación de ambos, puede tener consecuencias graves para el bienestar de los ciudadanos, para nuestras economías y para la confianza en nuestros sistemas democráticos*[8].

- Como corolario del trabajo y actividades de la Comisión Europea se presentan recomendaciones a los países signatarios, con el fin de avanzar en la elaboración de estrategias nacionales para la protección de ICE. La prioridad converge en el reforzamiento y resiliencia de sectores y áreas vitales identificadas como:

> *"… energía, la infraestructura digital, el sector del transporte y el espacial, y cuando sea posible en aquellos sectores incluidos en el ámbito de aplicación de la nueva Directiva REC, a saber, la banca, las infraestructuras de los mercados financieros, la infraestructura digital, la salud, el agua potable, las aguas residuales, las administraciones públicas, el espacio y la producción, transformación y distribución de alimentos, teniendo en cuenta la posible naturaleza híbrida de las amenazas, incluidos los efectos en cascada y los efectos del cambio climático"*[9].

- El resultado de este proceso ha sido, entre otras, la elaboración de estrategias para la protección de IC nacionales. De esta manera, la mayoría de los países signatarios poseen instrumentos normativos que establecen roles, funciones, así como una estructura institucional para la protección de la IC a la luz de riesgos y amenazas.

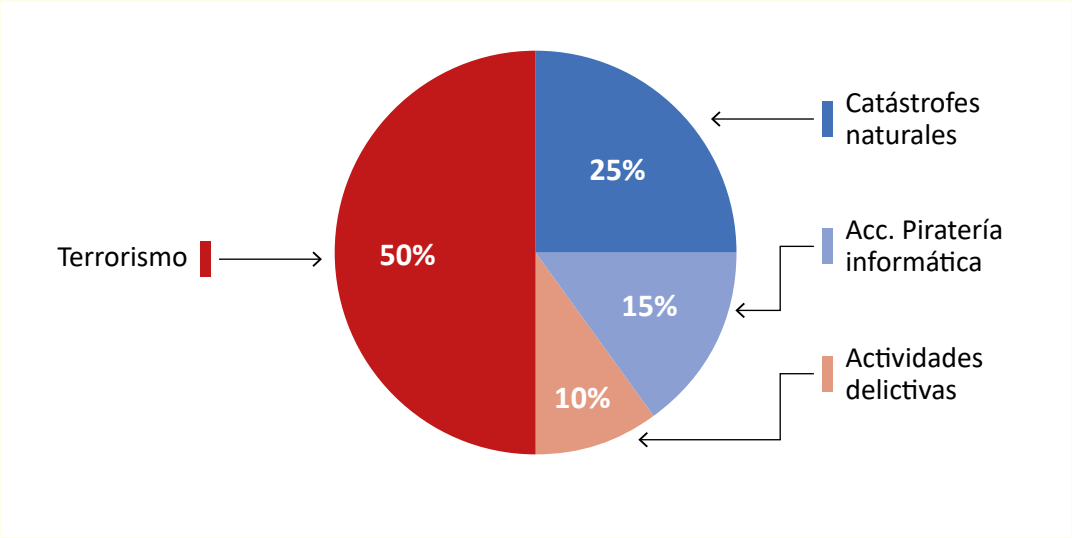
---

7 Ibid.

8 COMISIÓN EUROPEA. "*Sobre un enfoque coordinado de la Unión para reforzar la resiliencia de las infraestructuras críticas".* Estrasburgo, 18.10.2022. p. 1. En: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52022DC0551

9 Ibid. pp. 14–22.

Gráfico 1
Elementos perturbadores, riesgos y amenazas a la IC en porcentaje de preponderancia



Fuente: Elaboración propia en base a documentos base de la Comisión Europea (2008 y 2022).

Cuadro 1
Sectores estratégicos de Infraestructura Crítica

Sector		Servicios
I	Energía	- Producción, refinación, tratamiento y almacenamiento de petróleo y gas, incluyendo tuberías. - Generación eléctrica. - Transmisión de electricidad, gas y petróleo. - Distribución de electricidad, gas y petróleo.
II	Tecnologías, Comunicación e Información (TIC)	- Sistema de información y protección de redes. - Sistemas de automatización y control de instrumentación (SCADA, etc.) - Internet. - Provisión de telecomunicaciones fijas. - Provisión de telecomunicaciones móviles. - Radiocomunicación y navegación. - Comunicación por satélite - Radiodifusión
III	Agua	- Provisión de agua potable. - Control de la calidad del agua. - Destilado y control de cantidad de agua.

IV	Alimentación	- Suministro de alimentos y salvaguardia de la inocuidad y protección de los alimentos
V	Salud	- Atención médica y hospitalaria. - Medicamentos, sueros, vacunas y productos farmacéuticos. - Biolaboratorios y bioagentes.
VI	Financiero	- Servicios de pago/estructuras de pago (privadas). - Asignación financiera del gobierno.
VII	Orden y Seguridad Pública y Legal	- Mantener el orden público y legal, la seguridad y la protección. - Administración de justicia y detención.
VIII	Administración Civil	- Funciones gubernamentales. - Fuerzas Armadas. - Servicios de administración civil. - Servicios de emergencia. - Servicios postales y de mensajería.
IX	Transporte	- Transporte por carretera. - Transporte ferroviario. - Tráfico aéreo. - Transporte por vías navegables interiores. - Transporte marítimo y marítimo de corta distancia.
X	Industria química y nuclear.	- Producción y almacenamiento/procesamiento de productos químicos y sustancias nucleares. - Tuberías de mercancías peligrosas (sustancias químicas)
XI	Espacio e investigación	- Espacio. - Investigación.

Fuente: Libro Verde Comisión de las Comunidades Europeas, 2005. (Traducción propia)

- **Del proceso de decodificación nacional**

- Una de las aproximaciones más afines que, para este estudio resulta relevante, constituye el informe "Infraestructura Crítica para el Desarrollo" (ICD) 2016-2025, de la Cámara Chilena de la Construcción (CChC)[10]. Dicho documento, junto con actualizar la versión anterior, incorpora nuevos elementos de análisis como los cambios macroeconómicos globales y políticos locales, un entorno que ha modificado la agenda de desarrollo; por otra parte, examina las vulnerabilidades estructurales nacionales, esta vez, desde la perspectiva territorial. Finalmente, en su metodología aplica estándares más elevados que permiten vigencia de sus contenidos. En síntesis, se enfatiza

10 CChC. Cámara Chilena de la Construcción. Informe Infraestructura Crítica para el Desarrollo (ICD) 2016-2025. 6 de abril de 2016. p. 6. [Fecha de consulta: 15 de mayo de 2024] Disponible En: http://www.cchc.cl/uploads/archivos/archivos/Infraestructura-Critica-para-el-Desarrollo_2016-2025.pdf

una división de esferas, consideradas fundamentales, para el desarrollo nacional al establecer:

> *"…doce sectores clave para el progreso social y económico del país, agrupados en tres ejes estratégicos: infraestructura que nos sostiene o basal (agua, energía y telecomunicaciones), infraestructura que nos conecta o de apoyo logístico (vialidad interurbana, aeropuertos, puertos y ferrocarriles) e infraestructura que nos involucra o de uso social (vialidad urbana, espacios públicos, educación, hospitales y cárceles)"*[11].

- El mérito de la publicación se sustenta en alertar a diferentes autoridades y sectores productivos sobre la necesidad de diseñar estrategias para el desarrollo nacional. Los ejes se fundamentan en la necesidad de generar políticas para un progreso viable y eficiente, e impulsar un plan de inversiones que busque soluciones rentables y sostenibles en el tiempo respecto de las problemáticas actuales. Sin embargo, llama la atención la ausencia de la amenaza antrópica como componente de análisis. Una variable que irrumpe con mayor fuerza en diferentes escenarios, y que la OCDE ya lo incorporó.

- Sin embargo, la temática posee una extensa data de normas que han incorporado variables de afectación de IC, las que han sido abordadas acorde a contextos o bien experiencias nacionales. El relato se encuentra reflejado en el Mensaje n° 122-371 de S.E. el Presidente de la República al Senado, que propone a trámite una norma destinada a la protección de IC nacional, presentando los siguientes antecedentes[12]:

  - Decreto Ley N° 3.607 (1981), del Ministerio del Interior que establece nuevas normas sobre funcionamiento de vigilantes privados, haciendo mención a empresas estratégicas.

  - Ley N° 18.168 (1982), General de Telecomunicaciones, en el Cap. VII "De las Infraestructuras Críticas de Telecomunicaciones".

  - Ley N° 20.478 (2011), sobre recuperación y continuidad en condiciones críticas y de emergencia del sistema público de telecomunicaciones.

  - Decreto 60 (2012), del Ministerio de Transportes y Telecomunicaciones, el que establece un reglamento para la interoperación y difusión de la mensajería de alerta, declaración y resguardo de la infraestructura crítica de telecomunicaciones e información.

- Por otra parte, el 2018 se publica la Política de Ciberdefensa (PCD)[13]. Dicho instrumento normativo busca establecer la debida protección a la IC de la información,

11 Ibid.

12 MENSAJE Nº 122-371 "*Proyecto de ley, iniciado en Mensaje de S.E. el Presidente de la República para la protección de la infraestructura crítica del país*". 01 agosto, 2023. En: https://www.doe.cl/alerta/04082023/20230804034

13 LEY Nº 42.003. Política de Ciberdefensa. Ministerio de Defensa Nacional. 9 de marzo de 2018. [en línea] [Fecha de consulta: 15 de mayo de 2024] Disponible En: http://www.diariooficial.interior.gob.cl/publicaciones/2018/03/09/42003/01/1363153.pdf

en este caso, desde la lógica de la Defensa Nacional. Dimensión que requería estar sintonizada con el articulado promulgado para el ámbito de la Ciberseguridad. Este último cuerpo legal describe:

> *"Dentro de las infraestructuras de la información, existe un conjunto especialmente relevante para la marcha del país, las denominadas infraestructuras críticas de la información (ICI), que comprende las instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya afectación, degradación, denegación, interrupción o destrucción pueden tener una repercusión importante en la seguridad, la salud, el bienestar de los ciudadanos y el efectivo funcionamiento del Estado y del sector privado"*[14].

- La administración gubernamental, a través de los documentos señalados, procura establecer una separación inequívoca respecto de la IC de la información, sin embargo no concluye sobre el alcance y efectos que se ciernen sobre la IC en particular, al establecer:

> *"En el caso chileno, mientras se adopta una política específica para infraestructuras críticas, la infraestructura de la información de los siguientes sectores será considerada como crítica: energía, telecomunicaciones, agua, salud, servicios financieros, seguridad pública, transporte, administración pública, protección civil y defensa, entre otras".*
>
> *"Por otra parte, deberá evaluarse la pertinencia de crear un Computer Security Incident Response Team, (CSIRT), de infraestructuras críticas"* [15].

- La preocupación gubernamental por establecer lineamientos sobre IC con el fin de sincronizar en toda su extensión, a través de diferentes normativas legales, también ha contribuido en retardar su aplicabilidad por parte de los actores involucrados, sean públicos o privados. A mayor abundamiento, mediante la promulgación de la nueva Política Nacional de Ciber Seguridad (PNCS) el país recoge el principio señalado por el Art. 51 de la Carta de Naciones Unidas, otorgando un nivel superlativo al dominio del internet. El problema se sitúa en el grado de responsabilidad que le compete a quien provee el servicio, cuando éstos son privados, al señalar:

> *"… Este principio pone la infraestructura de comunicaciones de Internet al mismo nivel que la infraestructura considerada estratégica y vital para el país, como la red de transporte y la red de centros de salud, entre otros"*[16].

- En línea con lo ya prescrito, la Política de Defensa Nacional 2020 (PDN) enfatiza sobre las amenazas a las que se enfrenta el país, y en lo pertinente a la IC establece:

---

14 PNCS. Política Nacional de Ciber Seguridad, 2017-2022. p. 16. https://biblioteca.digital.gob.cl/server/api/core/bitstreams/b5b26f36-2c47-441b-8848-00d767ec9b5c/content

15 Ibid. p. 17.

16 PNCS. Política Nacional de Ciber Seguridad, 2023–2028. p. 7. https://www.diariooficial.interior.gob.cl/publicaciones/2023/12/04/43717/01/2415658.pdf

> *"En el caso de Chile, cobra relevancia para la seguridad nacional la protección de las infraestructuras críticas de información asociadas a servicios esenciales para el país, cuya paralización o uso con fines maliciosos puede afectar gravemente a nuestra población. Una agresión de este nivel puede ser calificada como un acto hostil que podría configurar el derecho a legítima defensa"*[17].

- Finalmente, frente a una serie de eventos perturbadores para la seguridad interna, cuya expresión más álgida se constató durante el último lustro, la autoridad política resuelve autorizar el empleo de las Fuerzas Armadas para permitir la protección de la IC, en caso de peligro grave o inminente, prescribiendo:

> *"La infraestructura crítica comprende el conjunto de instalaciones, sistemas físicos o servicios esenciales y de utilidad pública, así como aquellos cuya afectación cause un grave daño a la salud o al abastecimiento de la población, a la actividad económica esencial, al medioambiente o a la seguridad del país"* [18].

- Dado el amplio espectro establecido se colige que mientras no se adopte una política nacional que instaure el marco de acción y regulatorio para la protección de la IC, se mantendrá el dilema respecto de quién hace qué. Además, se constata una preeminencia de misiones, roles y cometidos de las FF. AA. en ámbitos que le son ajenos a su función principal. En este estado de las cosas resulta imprescindible identificar las estructuras vitales que requieren y deben ser protegidas, para luego avanzar en el diseño de una gobernanza del sistema.

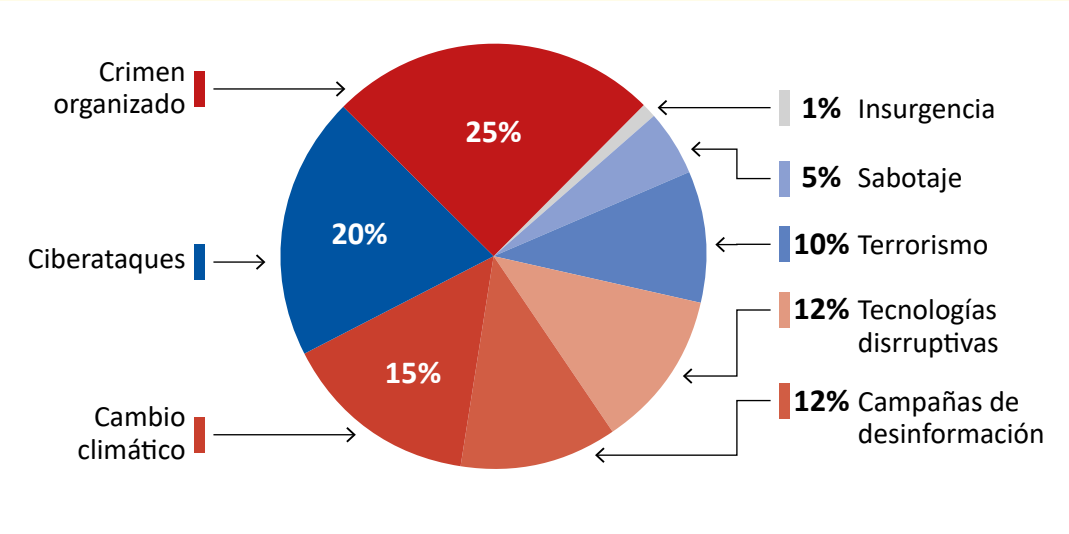
- Como resultado del proceso nacional, entre otras, ha sido la elaboración de documentos normativos cuyo objetivo ha sido abordar la temática de la IC de forma parcial o compartimentada. Pese a la transversalidad que ofrece el concepto no se identifica una estructura de gestión para la protección de sectores vitales y áreas sensibles, menos aún una estrategia que guie fórmulas y métodos para la protección de la IC a la luz de incidentes que se han manifestado con devastadoras consecuencias.

- En gráfico 2 y cuadro 2, respectivamente, se aprecia la magnitud de las amenazas, en términos de mayor incidencia perturbadora, que han afectado las estructuras nacionales y, del mismo modo, densidad normativa en que se ha abordado la codificación y sistematización de IC.

17 PDN. 2020. pp. 43–49. En: https://www.defensa.cl/wp-content/uploads/2023/06/POLÍTICA-DE-DEFENSA-NACIONAL-DE-CHILE-2020.pdf

18 BCN. Ley Nº 21.542. Loc. Cit.

Gráfico 2
Elementos perturbadores y amenazas a la IC de Chile en porcentaje de priorización



Fuente: Elaboración propia basado en Política de Defensa Nacional de Chile (2020) e incidencias de afectación.

Cuadro 2
Sectores de estratégicos de Infraestructura Crítica

Sector		Servicios
I	Energía, gas, agua	- Generación. - Transmisión. - Transporte. - Producción. - Almacenamiento. - Distribución.
II	Conexión vial, aérea, terrestre, portuaria o ferroviaria	- Conjunto de instalaciones. - Sistemas físicos. - Servicios esenciales
III	Servicios de utilidad pública (Asistencia sanitaria)	- Atención médica y hospitalaria. - Servicios esenciales.

Fuente: Elaboración propia basado en Ley Nº 21.542 de 3 de febrero, 2023.

- **Cotejando *IC nacionales a partir de lo establecido por la OCDE*[19]**

Como se ha señalado, para la OCDE el concepto "crítico" se refiere a instalaciones que, si se inutilizaran o destruyeran, provocaría daños catastróficos y de gran alcance afectando el desarrollo y bienestar. Por lo amplio del espectro conceptual, varios países concurrentes han establecido un catálogo de infraestructuras a las que el Estado debe proteger.

De esta manera, del análisis a los documentos publicados por la organización, se pueden identificar aquellas áreas estratégicas en que diferentes niveles de autoridades poseen atributos y responsabilidades para su resguardo. En palabras simples, se ha diseñado un sistema de protección de IC, estratificando áreas sensibles y sectores estratégicos para gestionar la respectiva protección. El cuadro 3 permite cotejar el listado de sectores críticos:

Cuadro 3
Cotejo de sectores esenciales e IC

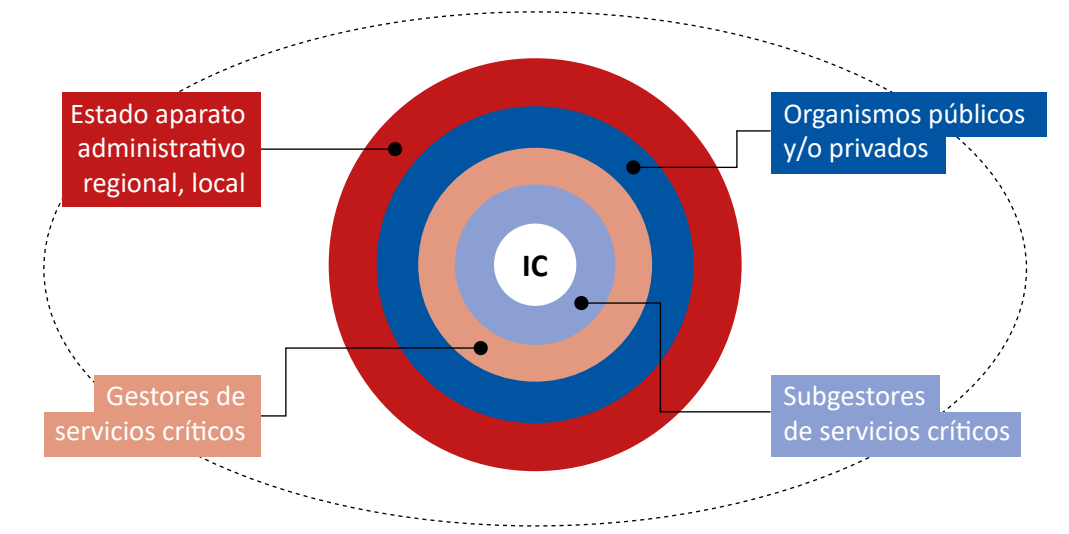
Comunidad Europea (Recomendaciones Comisión)	**OCDE Normas de IC**	**Chile (Políticas que refieren a IC)**
Energía	Energía	Energía (Electricidad, gas) **Ley nº** 21.542
Tecnologías, Comunicación e Información (TIC)	Comunicaciones, radio, televisión, correos	Tecnologías, Comunicación e Información (TIC) **Ley n° 18.168 – nº 20.478** (**PNCS**)
Agua	Agua y tratamiento	Agua **Ley nº** 21.542
Alimentación	Agricultura y alimentación	NO
Salud	Salud	Salud **Ley nº** 21.542
Financiero	Banca y finanzas	**Circular Bancos nº 2261** **CMF Resolución n°**3255
Orden y Seguridad Pública y Legal	Defensa	Ciberdefensa (**PCD**)
Administración Civil	NO	NO

19 OCDE. "*Protection of "critical infrastructure" and the role of investment policies relating to national security*". 2008. En: https://www.oecd.org/investment/investment-policy/40700392.pdf

Transporte	Transporte	Transporte (vial, aéreo, terrestre, portuario, ferroviario) **Ley nº** 21.542 **Decreto nº** 60
Industria química y nuclear	Industria química y petrolera	NO
Espacio e investigación	Transversales	NO

Fuente: Elaboración propia. Resumen conclusivo.

Imagen 1
Sistematización de gestores de protección de IC.



Fuente: Elaboración propia.

Conclusiones

Las diferentes aproximaciones conceptuales, normativas y metodológicas, que se han analizado apuntan a establecer que las IC se vinculan con instalaciones y sistemas que proveen servicios esenciales para un Estado. En dicha condición, su destrucción, alteración o mal funcionamiento provocarían afectaciones de amplio espectro. Este socavamiento se produce tanto en espacios individuales, organizacionales y estructurales, generando una brecha de vulnerabilidad a la seguridad nacional.

Considerando el espectro señalado, las IC establecidas por países signatarios de la OCDE y Comunidad Europea se identifican y agrupan de acuerdo al grado de sensibilidad, así como en sectores estratégicos. Dichos sectores constituyen parte medular de un mapa de riesgos y amenazas establecidas por el Estado. Por consiguiente, se precisa de una adecuada y actualizada inteligencia para la oportuna toma de decisiones de nivel central.

Para una adecuada gestión de la estratificación sectorial de la IC, y su consecuente delegación de responsabilidades, la experiencia acumulada por países de la Comunidad Europea, así como integrantes de la OCDE, se constata una preeminencia de un diseño de gestión centralizado en su control (Estado) y descentralizado para la ejecución (actores del sistema).

En el caso nacional, si bien se ha avanzado en normativas de protección de la IC y discusión de temáticas afines, se confirma que los instrumentos no logran generar una sincronización de la gestión de protección de IC. Esta condición se origina, principalmente, por la amplitud y ambigüedad de criterios que intentan abordar desde diferentes ordenanzas su conceptualización; por otra parte, a la falta de un catastro sectorial de estructuras sensibles y, finalmente, a la inexistencia de una fórmula que permita el control y coordinación de los actores del sistema. En otras palabras, la ausencia de un plan maestro y estrategias para la protección de la IC Nacional.

La fórmula establecida por la autoridad, conforme a la Ley Nº 21.542 y lo propuesto en el Mensaje Nº 122-371, deposita en las FF. AA. e instituciones de seguridad y policiales una prerrogativa superlativa para la protección de la IC. Dicho entorno se mantendrá hasta que no se diseñe una gobernanza que sincronice a los diferentes actores y servicios del sistema, sean públicos o privados. Así las cosas, las instituciones de la defensa y de seguridad podrían destinarse al resguardo de supermercados, farmacias, bancos o estaciones de combustible, antenas de radiocomunicación, entre otras instalaciones de carácter privado que se identifican como de alta sensibilidad o estratégicas.

La sensibilidad descrita requiere de normas explícitas, no solo para asegurar el actuar y empleo de la fuerza de instituciones encargadas del orden público o de defensa nacional, sino que demanda el desarrollo de capacidades de organismos civiles y del propio aparato público, tal como lo prescribe la CChC en su segundo informe.

La comunidad académica, en su rol de gestión del conocimiento y vinculación social, puede y debe contribuir significativamente en propuestas de políticas que faciliten una eficaz decodificación de la IC que impulse a superar las vulnerabilidades y brechas de las normativas evidenciadas. La base científica de estudios, promovida por investigadores especializados, constituyen un estadio de reconocida fuente de retroalimentación. Un entorno que, por ahora, se observa alejado de la discusión.

REFERENCIAS BIBLIOGRÁFICAS

BCN. "Circular Bancos *2261. Recopilación actualizada de normas"*. Capítulos 1-13 y 20-10 Gestión de la seguridad de la información y ciberseguridad. [en línea] [Fecha de consulta: 26 de mayo de 2024] En: https://www.bcn.cl/leychile/navegar?i=1150515&f=2020-07-06

BCN. Ley Nº 21.542. "*Modifica la carta fundamental con el objeto de permitir la protección de infraestructura crítica por parte de las fuerzas armadas, en caso de peligro grave o* inminente". Febrero, 2023. [en línea] [Fecha de consulta: 11 de mayo de 2024] En: https://www.bcn.cl/leychile/navegar?idNorma=1188583

CChC. Cámara Chilena de la Construcción. "*Informe Infraestructura Crítica para el Desarrollo"* (ICD) 2016-2025. 6 de abril de 2016. Pág. 6. [Fecha de consulta: 15 de mayo de 2024] Disponible En: http://www.cchc.cl/uploads/archivos/archivos/Infraestructura-Critica-para-el-Desarrollo_2016-2025.pdf

CMF. Capítulo 20-10 "*Gestión de seguridad de la información y ciberseguridad*". 2020. En: https://www.cmfchile.cl/portal/principal/613/articles-29310_doc_pdf.pdf

COMISIÓN DE LAS COMUNIDADES EUROPEAS. Libro Verde. "*Sobre un programa europeo para la protección de infraestructuras críticas".* Bruselas. 17.11.2005. Anexo 1, p. 22. [en línea] [Fecha de consulta: 20 de mayo de 2024] En: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0576:FIN:ES:PDF

COMISIÓN EUROPEA. "S*obre un enfoque coordinado de la Unión para reforzar la resiliencia de las infraestructuras críticas".* Estrasburgo, 18.10.2022. p. 1. [en línea] [Fecha de consulta: 20 de mayo de 2024] En: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52022DC0551

COMISIÓN EUROPEA. "*Critical Infrastructure Protection in the fight against terrorism*". Brussels, 20.10.2004 COM (2004) 702 final, de 20 de octubre de 2004. En: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0702:FIN:EN:PDF

MENSAJE Nº 122-371. "*Proyecto de ley, iniciado en Mensaje de S.E. el Presidente de la República para la protección de la infraestructura crítica del país*". 01 agosto, 2023. En: https://www.doe.cl/alerta/04082023/20230804034

MINDEF. PDN. 2020. pp. 43–49. [en línea] [Fecha de consulta: 17 de mayo de 2024] En: https://www.defensa.cl/wp-content/uploads/2023/06/POLÍTICA-DE-DEFENSA-NACIONAL-DE-CHILE-2020.pdf

MINDEF. Ley Nº 42.003. Política de Ciberdefensa. 9 de marzo de 2018. [en línea] [Fecha de consulta: 15 de mayo de 2024] Disponible En: http://www.diariooficial.interior.gob.cl/publicaciones/2018/03/09/42003/01/1363153.pdf

OCDE. "*Recomendación del Consejo sobre la gobernanza de infraestructuras*", OECD/LEGAL/0460, p. 6, 2020. En: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0460

OECD. "*Recomendación del Consejo sobre la Gobernanza de Riesgos Críticos*". 6 de mayo de 2014. En: https://www.oecd.org/gov/risk/Critical-Risks-Recommendation-Spanish.pdf

PNCS. Política Nacional de Ciber Seguridad, 2017 - 2022. p. 16. [en línea] [Fecha de consulta: 15 de mayo de 2024] En: https://biblioteca.digital.gob.cl/server/api/core/bitstreams/b5b26f36-2c47-441b-8848-00d767ec9b5c/content

PNCS. Política Nacional de Ciber Seguridad, 2023–2028. p. 7. [en línea] [Fecha de consulta: 15 de mayo de 2024] En: https://www.diariooficial.interior.gob.cl/publicaciones/2023/12/04/43717/01/2415658.pdf

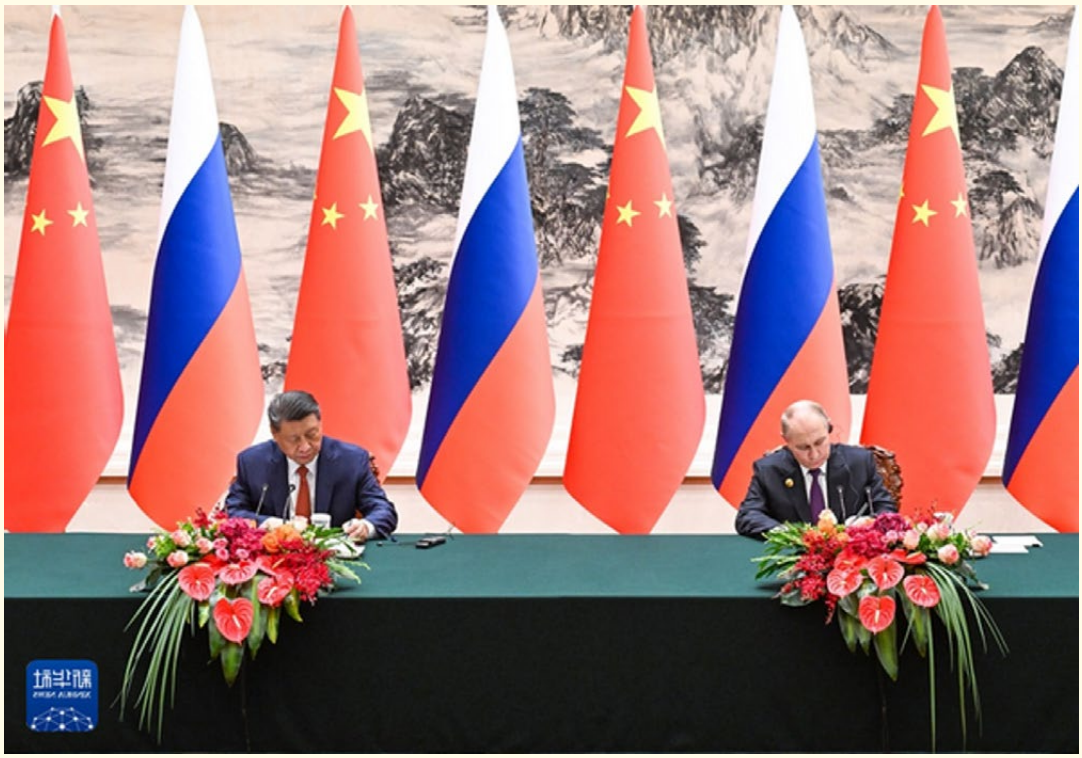
UE. Directiva 2008/114/CE del Consejo de la UE. "*Sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección"*. 8 diciembre 2008. [en línea] [Fecha de consulta: 20 de mayo de 2024] En: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32008L0114


ACADEMIA NACIONAL DE ESTUDIOS POLITICOS Y ESTRATEGICOS
CHILE

DOSSIER

EL ANUNCIO DE UN NUEVO ORDEN INTERNACIONAL

Declaración conjunta de la República Popular China y la Federación de Rusia sobre la profundización de la asociación estratégica de colaboración integral en la nueva era con motivo del 75º aniversario del establecimiento de relaciones diplomáticas entre los dos países



Por invitación del Presidente Xi Jinping de la República Popular China, el Presidente Vladimir Putin de la Federación Rusa realizó una visita de estado a la República Popular China los días 16 y 17 de mayo de 2024. Los dos jefes de estado mantuvieron conversaciones oficiales en Beijing y participaron conjuntamente en la Ceremonia de Apertura del Año de la Cultura Ruso-China 2024-2025 y en un concierto especial por el 75 aniversario del establecimiento de relaciones diplomáticas entre China y Rusia. El Primer Ministro Li Qiang del Consejo de Estado de la República Popular China se reunió con el Presidente ruso Vladimir Putin.

El presidente ruso, Vladimir Putin, viajó a Harbin para asistir a la ceremonia de inauguración de la 8ª Exposición China-Rusia.

La República Popular China y la Federación de Rusia (en adelante denominadas “las Partes”) declaran lo siguiente:

I

En 2024, China y la Federación de Rusia celebraron solemnemente el 75.º aniversario del establecimiento de relaciones diplomáticas entre los dos países. Durante 75 años, las relaciones entre China y Rusia han seguido un desarrollo extraordinario. La Unión Soviética fue el primer país del mundo en reconocer y establecer relaciones diplomáticas con la República Popular China. Después del colapso de la URSS, la República Popular China reconoció a la Federación de Rusia como sucesora legal de la URSS y reafirmó su voluntad de desarrollar las relaciones chino-rusas sobre la base de la igualdad, el respeto mutuo, el beneficio mutuo y la cooperación, y el Tratado. de Buena Vecindad. El Tratado de Buena Vecindad, Amistad y Cooperación entre la República Popular China y la Federación de Rusia, firmado el 16 de julio de 2001, ha sentado una base sólida para el fortalecimiento continuo e integral de las relaciones chino-rusas. El posicionamiento de las relaciones bilaterales ha mejorado continuamente, alcanzando el nivel más alto en la historia de la nueva era de asociación estratégica cooperativa integral. Gracias a los incansables esfuerzos de ambas partes, las relaciones entre China y Rusia han mantenido un desarrollo saludable y estable de acuerdo con los intereses nacionales de los dos países y el espíritu de buena vecindad y amistad constantes.

Las dos partes destacaron que las actuales relaciones chino-rusas han trascendido el modelo de alianza político-militar de la Guerra Fría y no están alineadas, no son conflictivas y no están dirigidas por terceros. Frente a la turbulenta y cambiante situación global, las relaciones entre China y Rusia han resistido la prueba de los vientos y las nubes internacionales y han puesto de relieve las cualidades de estabilidad y resiliencia, y se encuentran en el mejor nivel de la historia. Las dos partes enfatizan que el desarrollo de la asociación estratégica integral China-Rusia en la nueva era está en consonancia con los intereses fundamentales de los dos países y pueblos, no es una medida paliativa, no se ve afectado por una cosa ni por la otra, y tiene un fuerte impulso endógeno y valor independiente. Las dos partes defienden resueltamente sus derechos e intereses legítimos y se oponen a cualquier intento de obstruir el desarrollo normal de las relaciones entre los dos países, interferir en los asuntos internos de los dos países o restringir su espacio económico, tecnológico e internacional.

Las dos partes reafirman que China y Rusia siempre se han considerado socios prioritarios, siempre se han adherido al respeto mutuo, la igualdad de trato y la cooperación de beneficio mutuo, y siempre han cumplido escrupulosamente la Carta de las Naciones Unidas, el derecho internacional y las normas básicas del derecho internacional. relaciones, que sirvió de modelo para las relaciones entre los principales países del mundo y sus mayores vecinos. Las dos partes están dispuestas a profundizar aún más su cooperación estratégica integral, apoyarse firmemente mutuamente en cuestiones que afectan a sus intereses fundamentales, como la soberanía, la integridad territorial, la seguridad y el desarrollo, y hacer un uso racional y eficaz de sus respectivas ventajas con el objetivo de mantener la la seguridad y la estabilidad de sus respectivos países y promover su desarrollo y revitalización. Las dos partes seguirán los principios establecidos en el Tratado de Buena Vecindad, Amistad y Cooperación entre China y la Federación de Rusia firmado el 16 de julio de 2001, así como otros documentos y declaraciones bilaterales, y llevarán a cabo una cooperación de alta calidad y alto nivel. nivel y mutuamente beneficiosos en una amplia gama de áreas.

China acoge con satisfacción la celebración exitosa de las elecciones presidenciales en la Federación de Rusia en marzo de 2024 y cree que las elecciones fueron altamente organizadas, abiertas, objetivas y populares, y que los resultados demostraron plenamente que la política estatal adoptada por el gobierno ruso cuenta con un amplio apoyo y que El desarrollo de relaciones amistosas con la República Popular China es una parte importante de la política exterior de Rusia.

China condena enérgicamente a todos los organizadores, perpetradores y planificadores del inhumano ataque terrorista ocurrido en la región de Moscú el 22 de marzo de 2024, considera completamente inaceptable el ataque contra civiles y apoya a la parte rusa en su decidida lucha contra las fuerzas terroristas y extremistas y en mantener la paz y la estabilidad en el país.

La Federación de Rusia reafirma su adhesión al principio de una sola China, reconoce a Taiwán como parte inalienable de la República Popular China, se opone a cualquier forma de "independencia de Taiwán" y apoya firmemente las iniciativas de la parte china para salvaguardar la soberanía y la integridad territorial de la Estado y lograr la reunificación nacional. China apoya a la parte rusa en la salvaguardia de su seguridad, estabilidad, desarrollo y prosperidad, soberanía e integridad territorial, y se opone a la interferencia de fuerzas externas en los asuntos internos de Rusia.

Las partes señalan que la evolución de los grandes cambios en el mundo se está acelerando, el estatus y la fuerza de las potencias emergentes en los países y regiones del "Sur Global" están creciendo y la multipolaridad del mundo se está acelerando. Estos factores objetivos aceleraron la redistribución del potencial, los recursos y las oportunidades de desarrollo en favor de los mercados emergentes y los países en desarrollo, y contribuyeron a la democratización de las relaciones internacionales y la justicia internacional. Sin embargo, los países que adhieren al hegemonismo y a la política de poder se oponen a esto, tratando de reemplazar y subvertir el orden internacional universalmente reconocido basado en el derecho internacional por un "orden basado en reglas". Las dos partes enfatizan que el concepto de construir una comunidad de destino humano y una serie de iniciativas globales presentadas por China son de gran importancia.

Como fuerzas independientes en el proceso de construcción de un mundo multipolar, China y la Federación de Rusia explotarán plenamente el potencial de sus relaciones, promoverán la realización de un mundo multipolar igualitario y ordenado y la democratización de las relaciones internacionales, y unirán sus esfuerzos para construir un mundo multipolar. un mundo multipolar justo y racional.

Las partes creen que todos los países tienen derecho a elegir independientemente su propio modo de desarrollo y sistemas políticos, económicos y sociales de acuerdo con sus condiciones nacionales y los deseos de sus pueblos, y se oponen a la injerencia en los asuntos internos de los Estados soberanos, a las sanciones unilaterales y "jurisdicción de armas largas" que no tienen base en el derecho internacional y no están autorizadas por el Consejo de Seguridad, así como el trazado de líneas basadas en ideología. Ambas partes señalan que el neocolonialismo y la hegemonía son completamente contrarios a la tendencia actual de los tiempos y piden el diálogo en pie de igualdad, el desarrollo de asociaciones y la promoción de los intercambios y el entendimiento mutuo entre civilizaciones.

Las dos partes seguirán defendiendo firmemente la victoria en la Segunda Guerra Mundial y el orden mundial de posguerra consagrado en la Carta de las Naciones Unidas, y se opondrán a la negación, distorsión y falsificación de la historia de la Segunda Guerra Mundial. Las partes señalan la importancia de educar a la gente sobre la visión correcta de la historia, proteger las instalaciones del monumento mundial antifascista contra la profanación o destrucción y condenar severamente la glorificación e incluso los intentos de revivir el nazismo y el militarismo. Las dos partes planean conmemorar el 80º aniversario de la victoria en la Guerra de Resistencia del Pueblo Chino contra Japón y la Guerra Patriótica de la URSS en 2025, y promover conjuntamente una visión correcta de la historia de la Segunda Guerra Mundial.

II

Las dos partes utilizarán la diplomacia de jefes de Estado como guía para promover el desarrollo integral de la asociación estratégica integral de cooperación China-Rusia en la nueva era. Las dos partes implementarán plenamente el importante consenso alcanzado por los Jefes de Estado de los dos países, continuarán manteniendo estrechos intercambios de alto nivel, asegurarán el buen funcionamiento del mecanismo de intercambio gubernamental, local y privado, y estudiarán activamente la creación de nuevos canales de cooperación.

Las dos partes continuarán manteniendo intercambios entre los líderes de los órganos legislativos de los dos países, profundizarán la cooperación entre los comités parlamentarios de cooperación, grupos de trabajo conjuntos, comités especializados y grupos de amistad de parlamentarios de los dos países, mantendrán los intercambios y la cooperación entre el General La Oficina del Comité Central del Partido Comunista de China (PCC) y la Oficina General Presidencial de la Federación de Rusia llevan a cabo diálogos de confianza mutua en el marco del mecanismo de consultas estratégicas de seguridad y cooperación en materia de seguridad policial y promueven los intercambios entre partidos políticos. , así como entre la sociedad civil y la academia en ambos países.

Las partes se complacen en observar que los dos países han desarrollado constantemente la cooperación en materia de defensa basada en un alto nivel de confianza mutua estratégica, protegiendo efectivamente la seguridad regional y global. Las dos partes profundizarán aún más la confianza mutua y la cooperación en asuntos militares, ampliarán la escala de ejercicios conjuntos y actividades de entrenamiento, organizarán periódicamente cruceros conjuntos en el mar y en el aire, fortalecerán la coordinación y la cooperación en marcos bilaterales y multilaterales y mejorarán continuamente su desarrollo. capacidad y habilidad para enfrentar de manera conjunta desafíos riesgosos.

Las dos partes conceden gran importancia a la cooperación en el ámbito de la aplicación de la ley y la seguridad y están dispuestas a fortalecer la cooperación en la lucha contra el terrorismo, el separatismo, el extremismo y la delincuencia organizada transnacional en el marco de la cooperación bilateral, así como en el marco de las Naciones Unidas. la Organización de Cooperación de Shanghai (OCS) y los países BRICS. Las partes se comprometen a fortalecer la cooperación entre las autoridades policiales locales de los dos países en las zonas fronterizas.

Las Partes señalan que es inaceptable interferir en los asuntos soberanos de los Estados mediante el uso de jurisdicciones multilaterales o nacionales o la prestación de asistencia a jurisdicciones extranjeras o mecanismos legales multilaterales, y expresan su profunda preocupación por la creciente politización de la justicia penal internacional y la violación de los derechos humanos y las inmunidades soberanas. Las Partes consideran que la adopción de tales medidas por cualquier Estado o grupo es ilegal, viola normas universalmente reconocidas del derecho internacional y socava la capacidad de la comunidad internacional para combatir el crimen.

Las partes están convencidas de que, de conformidad con el principio fundamental del derecho internacional de la igualdad soberana de los Estados, deben observarse estrictamente las obligaciones internacionales relativas a la inmunidad de los Estados y sus bienes, incluidas las reservas soberanas. Las partes condenan los intentos de confiscar activos y propiedades extranjeras y enfatizan el derecho del Estado lesionado a tomar contramedidas de conformidad con el derecho internacional. Las partes están decididas a brindar protección a los bienes nacionales de la otra parte en sus países y a garantizar la seguridad, la inviolabilidad y el regreso oportuno de los bienes nacionales de la otra parte durante su transporte temporal a sus países.

Las Partes planean mejorar el mecanismo para el reconocimiento y la ejecución de sentencias judiciales previsto en el Tratado entre la República Popular China y la Federación de Rusia sobre asistencia jurídica mutua en asuntos civiles y penales del 19 de junio de 1992, firmado por la Federación de Rusia. y por la República Popular China.

Las Partes seguirán fortaleciendo la cooperación práctica en el ámbito de la gestión de emergencias, cooperarán en los ámbitos de prevención, mitigación, socorro y seguridad de catástrofes en el ámbito de la vigilancia espacial y las técnicas de rescate aéreo, y organizarán ejercicios y entrenamiento conjuntos de rescate.

III

Las partes creen que la cooperación práctica entre China y la Federación de Rusia es un factor importante para promover el desarrollo económico y social y la prosperidad común de los dos países, salvaguardar el progreso tecnológico y la soberanía económica de los países, modernizar los países y mejorar el bienestar de los pueblos. -ser y mantener la estabilidad y sostenibilidad de la economía mundial. Las partes están dispuestas a promover una globalización económica inclusiva. Las partes están satisfechas de que la cooperación práctica entre China y la Federación de Rusia en diversos campos continúe avanzando y logrando resultados positivos. Las partes están dispuestas a seguir profundizando la cooperación en diversos campos de acuerdo con el principio de beneficio mutuo y resultados beneficiosos para todos, trabajar juntos para superar los desafíos externos y los factores desfavorables, aumentar la eficiencia de la cooperación entre las partes y lograr estabilidad. y el desarrollo de alta calidad de la cooperación. A tal efecto, las partes acuerdan:

- De conformidad con la Declaración Conjunta del Presidente de la República Popular China y del Presidente de la Federación de Rusia sobre el Plan de Desarrollo de las Direcciones Prioritarias de la Cooperación Económica China-Rusia para el período hasta 2030, promover enérgicamente la realización de altos objetivos desarrollo de calidad de la cooperación en diversos campos.

- Ampliar continuamente la escala y optimizar la estructura del comercio bilateral, profundizar la cooperación en las áreas de comercio de servicios, comercio electrónico, economía digital y desarrollo sostenible, y mantener conjuntamente la estabilidad y seguridad de la cadena de suministro de la cadena industrial.

- Acoger con satisfacción la celebración de la octava Exposición China-Rusia en Harbin, China, y apoyar la participación de representantes de todos los ámbitos de la vida en China y Rusia en importantes foros y exposiciones organizados en los dos países.

- Elevar continuamente el nivel de cooperación en materia de inversión entre los dos países, promover conjuntamente la implementación de importantes proyectos de cooperación, proteger los derechos e intereses de los inversores y crear condiciones justas y equitativas para la inversión. Desempeñar activamente el papel de mecanismo de coordinación en el ámbito de las inversiones entre los dos países. Actualizar el Acuerdo entre el Gobierno de la República Popular China y el Gobierno de la Federación de Rusia sobre la Promoción y Protección Mutua de Inversiones lo antes posible.

- Acelerar la formulación y aprobación de una nueva versión del Proyecto de Plan de Cooperación en Inversiones China-Rusia en 2024, hacer todos los esfuerzos posibles para promover la implementación del Proyecto y mejorar la eficacia de la cooperación bilateral en inversiones.

- Consolidar y lograr continuamente un alto nivel de desarrollo de la cooperación energética estratégica entre China y Rusia para garantizar la seguridad económica y energética de los dos países. Esforzarse por garantizar la estabilidad y sostenibilidad del mercado energético internacional y mantener la estabilidad y resiliencia de la cadena de suministro del sector energético global. Llevaremos a cabo la cooperación en las áreas de petróleo, gas natural, gas natural licuado (GNL), carbón y electricidad de acuerdo con los principios del mercado, aseguraremos el funcionamiento estable de la infraestructura transfronteriza relevante y aseguraremos el flujo sin obstáculos del transporte de energía. Promover conjuntamente la implementación de proyectos energéticos a gran escala por parte de empresas chinas y rusas y profundizar la cooperación en áreas prospectivas como la energía renovable, la energía del hidrógeno y el mercado del carbono.

- Sobre la base de la experiencia de proyectos exitosos y en curso, profundizar la cooperación en el campo de la energía nuclear civil de acuerdo con los principios de beneficio mutuo y situación de beneficio mutuo e intereses equilibrados, incluida la fusión termonuclear, los reactores de neutrones rápidos y el ciclo cerrado del combustible nuclear. y explorar la cooperación en la parte inicial del ciclo del combustible nuclear y la construcción conjunta de centrales nucleares en un enfoque de paquete.

- Incrementar la participación de la moneda local en el comercio bilateral, el financiamiento y otras actividades económicas. Mejorar la infraestructura financiera de los dos países y facilitar los canales de liquidación para entidades comerciales entre los dos países. Fortalecer la cooperación regulatoria en los sectores bancario y de seguros de Rusia y China, promover el sano desarrollo de las instituciones bancarias y de seguros abiertas por las dos partes en los territorios de la otra parte, fomentar la inversión bilateral y emitir bonos en los mercados financieros del otro país con base

en el mercado. principios orientados. Apoyar una mayor cooperación en el ámbito de los seguros y reaseguros, así como en el ámbito de la mejora de la comodidad de los pagos, y crear condiciones favorables para el crecimiento de los volúmenes de turistas de ambas partes. Sobre la base del reconocimiento mutuo de las normas contables chinas y rusas (en el campo de la emisión de valores), las normas de auditoría y la supervisión de auditoría, promover activamente la cooperación mutuamente beneficiosa en áreas prácticas.

- Cooperación en materia de inteligencia financiera entre China y Rusia, prevención conjunta del lavado de dinero y financiación del terrorismo y otros riesgos, y fortalecimiento continuo de la colaboración en el marco multilateral contra el lavado de dinero.

- Elevar el nivel de cooperación en campos industriales e innovadores, desarrollar conjuntamente industrias avanzadas y fortalecer la cooperación tecnológica y productiva, incluida la industria manufacturera de aviación civil, la construcción naval, la fabricación de automóviles, la fabricación de equipos, la industria electrónica, la metalurgia, la minería del hierro, la industria química y la industria forestal. . Crear condiciones favorables para la implementación de prospectivos proyectos en áreas prioritarias, ampliar el intercambio comercial de productos industriales e incrementar su participación en el comercio bilateral, además de contribuir al proceso de modernización de las industrias de ambos países.

- Desarrollar una cooperación mutuamente beneficiosa en el campo de las tecnologías de la información y las comunicaciones, incluida la inteligencia artificial, las comunicaciones, el software, el Internet de las cosas, el código abierto, la seguridad de las redes y los datos, los videojuegos, la coordinación de radiofrecuencias, la educación vocacional y la investigación científica especializada.

- Consolidar la asociación a largo plazo entre las dos partes en el campo espacial, implementar los principales proyectos del programa espacial nacional en interés común de Rusia y China, promover la cooperación en el campo de la exploración lunar y del espacio profundo, incluida la construcción de estaciones internacionales. investigación lunar y fortalecer la cooperación en la aplicación de los sistemas de navegación por satélite Beidou y GLONASS.

- Liberar el enorme potencial de cooperación en el sector agrícola, ampliar el acceso mutuo a los mercados para los productos agrícolas de los dos países y elevar el nivel del comercio de soja y sus productos procesados, carne de cerdo, productos acuáticos, cereales, aceites y grasas, frutas y verduras. y frutos secos, así como otros productos agrícolas y alimentarios. Profundizaremos la cooperación en inversión agrícola y continuaremos estudiando el establecimiento de zonas piloto de demostración para la cooperación agrícola entre China y Rusia en el Lejano Oriente ruso y otras regiones.

- Profundizar la cooperación en transporte, logística y cruces fronterizos, construir corredores de transporte y logística estables, fluidos y sostenibles, y desarrollar rutas directas de transporte o tránsito entre los dos países. Al mismo tiempo, fortalecer la construcción de infraestructura de cruces fronterizos, mejorar la gestión estanda-

rizada de los cruces fronterizos, mejorar la eficiencia de la capacidad de inspección y despacho de cruces fronterizos y garantizar un flujo bidireccional estable y fluido de pasajeros y mercancías. Mejorar el despacho de aduanas y la capacidad de transporte de los trenes China-UE que transitan por Rusia garantizará conjuntamente un transporte de carga seguro y eficiente. Basándonos en la importancia estratégica de la asociación ruso-china, promoveremos activamente el desarrollo del transporte aéreo y alentaremos a las aerolíneas de ambas partes a aumentar el número de vuelos en más rutas de manera estandarizada para cubrir más regiones.

- Fortalecer la cooperación en el área aduanera, con foco en promover los intercambios y la cooperación en el área de comercio internacional de la "Ventanilla Única", aplicando mecanismos regulatorios modernizados y procesos de gestión automatizados, promoviendo aún más los intercambios comerciales, aumentando la transparencia de las operaciones de importación y exportación y combatiendo eficazmente violaciones aduaneras.

- Fortalecer el intercambio de experiencias y prácticas en la protección y aplicación de los derechos de propiedad intelectual y desempeñar plenamente el importante papel de los derechos de propiedad intelectual en la promoción de la innovación científica y tecnológica y el desarrollo económico y social.

- Fortalecer la cooperación mutuamente beneficiosa en el campo de la política de competencia, incluida la cooperación en la aplicación y protección de las reglas de competencia en los mercados de productos básicos (incluidos los mercados digitales de productos básicos), a fin de crear condiciones favorables para la cooperación económica y comercial entre las dos partes.

- Promover aún más la cooperación en industria, infraestructura, vivienda y desarrollo urbano.

- Establecer un subcomité sobre cooperación China-Rusia en las rutas marítimas del Ártico en el marco del mecanismo del Comité de Reuniones Ordinarias de Primeros Ministros ruso-chinos para llevar a cabo una cooperación mutuamente beneficiosa en el desarrollo y utilización del Ártico, proteger los ecosistemas de la región Ártico, promover el desarrollo de las rutas marítimas del Ártico como un importante corredor de transporte internacional. Alentar a las empresas de los dos países a fortalecer la cooperación en áreas como el aumento del volumen de tráfico en las rutas marítimas del Ártico y la construcción de logística de rutas. Rutas marítimas del Ártico Alentar a las empresas de ambos Los países fortalecerán la cooperación para aumentar la capacidad de las rutas marítimas del Ártico y construir infraestructura logística en las rutas marítimas del Ártico. Profundizar la cooperación en tecnología y construcción de barcos polares.

- Apoyar activamente la cooperación local y fronteriza y ampliar los intercambios locales integrales entre los dos países. Fortalecer la cooperación en materia de inversiones de acuerdo con los principios de comercialización y comercialización en el marco del régimen preferencial para el Lejano Oriente ruso y llevar a cabo la producción cooperativa en los sectores industrial y de alta tecnología. Desarrollar conjuntamente la Isla Heixiazi (Isla Mayor Ussuri) siguiendo los principios de buena vecindad y

respeto a la soberanía nacional. Acelerar las consultas sobre el texto del (proyecto) de acuerdo intergubernamental sobre la navegación de buques rusos y chinos en las aguas que rodean la zona de la isla Heixiazi (islas Tarabarov y Bolshoi Ussuriysky). Las partes entablarán un diálogo constructivo con la República Popular Democrática de Corea sobre la navegación de buques chinos en el curso inferior del río Tumen.

- Profundizar la cooperación en protección ambiental y fortalecer la cooperación en las áreas de protección de aguas transfronterizas, enlace en respuesta de emergencia a la contaminación ambiental, protección de la biodiversidad y eliminación de desechos sólidos.

- Continuar la estrecha colaboración para mejorar la calidad ambiental en las zonas fronterizas de los dos países.

- Continuar fortaleciendo la colaboración para implementar el Acuerdo de Cooperación Económica y Comercial entre la República Popular China y la Unión Económica Euroasiática, firmado el 17 de mayo de 2018, para promover la construcción conjunta de la Franja y la Ruta y la Unión Económica Euroasiática, y para Profundizar la cooperación y la conectividad en todos los aspectos en Asia y Europa. También profundizaremos la cooperación y la conectividad en todos los aspectos entre Asia y Europa.

- Continuaremos implementando el consenso de los dos Jefes de Estado sobre el desarrollo paralelo y coordinado de la "Franja y la Ruta" y la "Gran Asociación Euroasiática" y crearemos condiciones para el desarrollo económico y social independiente y estable de los países de Asia y Asia. Europa. Crear condiciones para el desarrollo económico y social independiente y estable de los países de Asia y Europa.

- Continuar la cooperación trilateral entre China, Rusia y Mongolia sobre la base de la Hoja de Ruta a Medio Plazo para el Desarrollo de la Cooperación Trilateral entre China, Rusia y Mongolia y el Plan Esquema para la Construcción del Corredor Económico China-Mongolia Rusia.

IV

Las partes creen que los intercambios humanísticos son de gran importancia y de gran alcance para mejorar el entendimiento mutuo, llevar adelante la tradición de buena vecindad, continuar la amistad entre los pueblos de los dos países durante generaciones y fortalecer la base social de las relaciones bilaterales. Las partes están dispuestas a realizar esfuerzos conjuntos para ampliar activamente la cooperación humanística entre los dos países, aumentar el nivel de cooperación y ampliar sus resultados. Para ello, ambas partes acordaron:

- Profundizar continuamente la cooperación educativa y mejorar la base legislativa. Promover los estudios bilaterales en el extranjero para ampliar la escala y mejorar la calidad, promover la enseñanza del chino en Rusia y del ruso en China, alentar a las instituciones educativas a ampliar los intercambios, administrar escuelas en cooperación, llevar a cabo capacitación conjunta de personal de alto nivel e investigaciones conjuntas, apoyar la cooperación. en el campo de la investigación básica entre universidades y facultades, apoyar las actividades de la Unión de Universidades del

Mismo Tipo y la Unión de Escuelas Secundarias, y profundizar la cooperación en educación vocacional y digital.

- Profundizar los intercambios científicos y tecnológicos. Utilizar el potencial de la cooperación en el campo de la investigación básica y aplicada, ampliando la cooperación dentro de la estructura de grandes instalaciones científicas, apoyando la construcción conjunta de laboratorios modernos y centros de investigación científica avanzados, manteniendo la iniciativa de desarrollo científico y tecnológico de los dos países, promoviendo intercambios de personal y realización de investigaciones interdisciplinarias sobre el cambio climático.

- Aprovechar al máximo las oportunidades del Año de la Cultura China-Rusia 2024-2025 para llevar a cabo intercambios integrales en las áreas de espectáculos culturales, museos, bibliotecas, preservación del patrimonio cultural, educación artística e industrias creativas. Ampliar la geografía de los intercambios culturales y promover activamente la participación de jóvenes y trabajadores culturales locales en Rusia y China. Continuaremos organizando festivales culturales, foros bibliotecarios y ferias culturales chino-rusas. Fomentamos el estudio de nuevas iniciativas, como el Concurso Internacional de Canción Popular. Las Partes creen que la diversidad y la singularidad de las culturas y civilizaciones son la base de un mundo multipolar y, sobre esta base, entablarán intercambios, cooperación y comprensión mutua y se opondrán a la politización de la cultura, la "doctrina de la superioridad de las civilizaciones". discriminatorias y excluyentes y la "eliminación de culturas" practicada por algunos países y pueblos. Oponerse a la politización de la cultura, a la discriminatoria y excluyente "doctrina de superioridad civilizatoria", a la "abolición cultural" practicada por algunos países y naciones, y a la destrucción y demolición de instalaciones monumentales y religiosas, y promover la aceptación de los valores morales tradicionales. por más países.

- Diálogo sobre la protección, estudio, reparación y uso de instalaciones históricas y religiosas, instalaciones de memoria de los mártires y patrimonio histórico y cultural.

- Promover la cooperación en el campo del cine, incluido el apoyo de China al establecimiento de la Academia Euroasiática de Cinematografía por parte de Rusia y la creación del Premio Abierto de Cine Euroasiático, y considerar activamente la selección de películas para participar en los premios pertinentes.

- Continuar promoviendo la cooperación en las áreas de medicina de desastres, enfermedades infecciosas, oncología y medicina nuclear, oftalmología, farmacología, salud maternoinfantil y otras áreas de atención médica. Aplicar experiencia avanzada en el campo de la tecnología médica moderna y promover la formación de talentos médicos superiores.

- Llevar a cabo la cooperación en el campo de la prevención y el control de enfermedades infecciosas, la transmisión de salud autóctona y transfronteriza, ampliar la cooperación en alerta temprana y respuesta a desastres biológicos, proteger la soberanía nacional de los dos países en el campo de la biología y otorgar gran importancia. importancia para el desarrollo de una cooperación relevante en las zonas fronterizas de Rusia y China.

- Evaluar con gran satisfacción los resultados del Año de Intercambios Deportivos China-Rusia 2022-2023, continuar promoviendo pragmáticamente la cooperación en el campo de los deportes y profundizar los intercambios en diversos programas. China valora mucho los primeros Juegos del Futuro que Rusia celebrará en Kazán en 2024 y apoya a la parte rusa en la organización de los Juegos BRICS. Las dos partes se oponen a la politización del deporte y a cualquier uso del deporte como herramienta para discriminar a los atletas por motivos de nacionalidad, idioma, religión, creencias políticas o de otro tipo, raza y origen social, y piden a la comunidad internacional que lleve a cabo la cooperación. deportes internacionales en pie de igualdad, de conformidad con el espíritu y los principios olímpicos.

- Ampliar la cooperación en el campo del turismo, crear condiciones favorables para aumentar el volumen de visitas mutuas de turistas chinos y rusos, promover el desarrollo del turismo transfronterizo, implementar conjuntamente el Acuerdo entre el Gobierno de la República Popular China y el Gobierno de Federación Rusa sobre Exención Mutua de Visas para Turismo de Grupo, firmado el 29 de febrero de 2000, y acelerar las negociaciones sobre la revisión del Acuerdo.

- Fortalecer los intercambios de medios entre los dos países, promover visitas mutuas a todos los niveles, apoyar diálogos pragmáticos y profesionales, desarrollar activamente la cooperación en contenidos de alta calidad, explorar profundamente el potencial de la cooperación en el campo de los medios de comunicación con los nuevos medios y las nuevas tecnologías, informa objetiva y exhaustivamente sobre acontecimientos clave en todo el mundo y difundir información veraz en el ámbito de la opinión pública internacional. Continuaremos promoviendo el intercambio de conocimientos y experiencias y la cooperación entre las organizaciones editoriales y de traducción de libros de los dos países, así como promoviendo la transmisión mutua de programas de canales de televisión.

- Apoyar la cooperación en el sector de archivos, incluido el intercambio de experiencias en trabajos avanzados e información de archivos, así como la preparación conjunta de publicaciones de archivos y la implementación de proyectos de exposición sobre la historia de Rusia y China y la historia de las relaciones entre los dos países. .

- Apoyar el trabajo del Comité Ruso-Chino para la Amistad, la Paz y el Desarrollo, fomentar la cooperación a través de los canales de asociaciones de amistad y otros grupos civiles de amistad, promover los intercambios civiles y el entendimiento mutuo entre China y Rusia, y fortalecer los intercambios entre los think tanks especializados de ambos. países.

- Fortalecer la cooperación en el ámbito de la juventud, llevar a cabo educación sobre ideales y creencias, valores correctos y patriotismo, y apoyar a los jóvenes en la innovación y el espíritu empresarial, el voluntariado y la mejora de la creatividad. Consolidar y enriquecer los resultados del Festival Mundial de la Juventud y el Foro Mundial de Desarrollo de la Juventud, continuar profundizando los intercambios juveniles en todos los niveles, colaborar en plataformas juveniles multilaterales y promover ideas comunes para la cooperación internacional.

V

Las dos partes reafirman su compromiso con la construcción de un sistema internacional multipolar más justo y estable, respetando y cumpliendo incondicional y plenamente los propósitos y principios de la Carta de las Naciones Unidas y defendiendo un multilateralismo genuino. Las Partes enfatizan la necesidad de fortalecer aún más el trabajo del Grupo de Amigos para la Defensa de la Carta de las Naciones Unidas.

Las dos partes están dispuestas a profundizar la cooperación bilateral dentro del marco de las Naciones Unidas, incluidas la Asamblea General y el Consejo de Seguridad, y a fortalecer su colaboración en la discusión de importantes cuestiones internacionales dentro de los diversos órganos de las Naciones Unidas.

Las dos partes están dispuestas a seguir realizando esfuerzos conjuntos para promover el diálogo constructivo y la cooperación en el ámbito de los derechos humanos a nivel multilateral, defender los valores comunes de toda la humanidad, oponerse a la politización de los derechos humanos, a los dobles raseros y el uso de cuestiones de derechos humanos para interferir en los asuntos internos de otros países, y promover conjuntamente el sano desarrollo de la agenda internacional de derechos humanos en todos sus aspectos.

Para mejorar la salud de toda la humanidad, las dos partes continúan trabajando estrechamente en cuestiones de salud global, incluido el apoyo al papel de la Organización Mundial de la Salud y oponiéndose a la politización de su trabajo.

Ambas partes están firmemente comprometidas con la promoción de un sistema comercial multilateral abierto, inclusivo, transparente y no discriminatorio, basado en las reglas de la Organización Mundial del Comercio. Las dos partes están dispuestas a fortalecer la cooperación en el marco de la OMC, impulsar la reforma de la OMC, incluido el restablecimiento del funcionamiento normal del mecanismo de solución de diferencias, y promover la implementación de los resultados de la 13ª Conferencia Ministerial de la OMC. Las partes se oponen a la politización de las relaciones económicas internacionales, incluido el trabajo de las organizaciones multilaterales en las áreas de comercio, finanzas, energía y transporte, lo que conducirá a la fragmentación del comercio mundial, el proteccionismo y la competencia desleal.

Las Partes condenan las acciones unilaterales que eluden el Consejo de Seguridad de las Naciones Unidas, violan el derecho internacional, incluida la Carta de las Naciones Unidas, y socavan la conciencia de justicia, así como las medidas unilaterales contrarias a las normas de la Organización Mundial del Comercio (OMC). Las medidas restrictivas que violan las reglas de la OMC impiden el desarrollo del libre comercio y tienen un impacto negativo en la cadena de suministro industrial global. China y la Federación de Rusia se oponen firmemente a ellas.

Además, las partes enfatizan su voluntad de fortalecer la colaboración en plataformas multilaterales en áreas especializadas, promover posiciones comunes y oponerse a la politización del trabajo de las organizaciones internacionales.

Las partes creen que la cooperación en el marco de la Organización de Cooperación de Shanghai (OCS) es una dirección importante para fortalecer la asociación estratégica

integral entre los dos países. Las dos partes continuarán sus esfuerzos de colaboración para transformar la Organización de Cooperación de Shanghai en una organización multilateral autorizada e influyente para que pueda desempeñar un papel más importante en la construcción de un nuevo panorama internacional multipolar, justo y estable.

Las dos partes trabajarán con otros estados miembros de la OCS para mejorar el trabajo de la organización, explorar el potencial de cooperación en las esferas política, de seguridad, económica y humana, y hacer de la región euroasiática un hogar común de paz, estabilidad, confianza mutua, desarrollo y prosperidad. .

China apoya plenamente la presidencia rusa de los BRICS en 2024 y la organización de la decimosexta reunión de líderes de los BRICS.

Las dos partes están dispuestas a trabajar con otros miembros del BRICS para implementar el consenso alcanzado en reuniones anteriores de líderes del BRICS, promover la integración de nuevos miembros al mecanismo de cooperación existente del BRICS y explorar modos de cooperación entre los países socios del BRICS. Las dos partes seguirán defendiendo el espíritu de los BRICS, realzando la voz del mecanismo de los BRICS en los asuntos internacionales y el establecimiento de la agenda internacional, y llevando a cabo activamente la cooperación BRICS+ y los diálogos periféricos de los BRICS.

Las dos partes promoverán la mejora de la colaboración BRICS en el ámbito internacional, incluido el fortalecimiento de la cooperación entre los países BRICS en las áreas de comercio, economía digital y salud pública, y al mismo tiempo, promoverán efectivamente el diálogo sobre el uso de la liquidación en moneda local. , herramientas de pago y plataformas para operaciones comerciales entre los países BRICS.

Ambas partes opinan que se debe fortalecer aún más el papel de la UNESCO como plataforma universal para los intercambios humanísticos intergubernamentales y que se deben promover diálogos profesionales y mutuamente respetuosos en la plataforma para facilitar la comunicación eficiente, el consenso y la solidaridad entre los Estados Miembros.

Las dos partes valoraron altamente la cooperación constructiva entre China y Rusia en el G20 y reafirmaron su voluntad de continuar fortaleciendo la cooperación en el marco del mecanismo, promover la construcción de una globalización económica inclusiva, tomar acciones equilibradas y consensuadas para enfrentar los desafíos económicos y los asuntos pendientes. cuestiones financieras, promover el desarrollo del sistema de gobernanza global en una dirección más justa y aumentar la representación de los países del “Sur Global” en el sistema de gobernanza económica global. Ambas partes dan la bienvenida a la Unión Africana como miembro del Grupo de los Veinte (G20). Las dos partes dan la bienvenida a la Unión Africana como miembro de pleno derecho del Grupo de los Veinte (G-20) y están dispuestas a trabajar de manera constructiva en beneficio de los mercados emergentes y los países en desarrollo.

Las dos partes continuarán desarrollando una cooperación estrecha y mutuamente beneficiosa dentro del marco de la Cooperación Económica Asia-Pacífico (APEC) para promover la implementación integral y equilibrada de la Visión Putrajaya y la construcción de una comunidad Asia-Pacífico. Con este fin, las dos partes están dispuestas a seguir promoviendo su posición común de principios sobre la construcción de una economía mundial

abierta, impulsando el proceso de integración económica regional en la región de Asia y el Pacífico, promoviendo la liberalización y facilitación del comercio y la inversión, garantizando la estabilidad y el flujo fluido de la cadena de suministro de la cadena industrial transfronteriza, y promover la transformación digital y verde y el desarrollo sostenible de la región de Asia y el Pacífico, en beneficio de los pueblos de la región.

La Federación de Rusia valora mucho la Iniciativa de Desarrollo Global (GDI) y seguirá participando en el trabajo del Grupo de Amigos de la GDI. Las dos partes seguirán alentando a la comunidad internacional a centrarse en las cuestiones de desarrollo, aumentar la inversión en desarrollo, profundizar la cooperación práctica y acelerar la implementación de la Agenda 2030 de las Naciones Unidas para el Desarrollo Sostenible.

VII

Las partes señalan que en la actualidad continúan los conflictos regionales y globales, el entorno de seguridad internacional es inestable y los riesgos estratégicos están aumentando como resultado de la intensificación de la confrontación entre Estados, incluidos los Estados que poseen armas nucleares. Las partes expresaron preocupación por la situación de seguridad internacional.

Las partes reafirman su compromiso con la Declaración conjunta de los líderes de los cinco Estados poseedores de armas nucleares sobre la prevención de la guerra nuclear y la prevención de una carrera armamentista del 3 de enero de 2022, en particular el concepto de que una guerra nuclear no se puede ganar ni es viable. y reiterar su llamado a todos los participantes en la Declaración Conjunta a aplicarla en la práctica.

Las dos partes creen que todos los estados poseedores de armas nucleares deben defender los principios de mantener la estabilidad estratégica global y la seguridad igual e indivisible, y no deben invadir los intereses vitales de cada uno mediante la expansión de alianzas y coaliciones militares y el establecimiento de bases militares cerca de las fronteras de otros Estados poseedores de armas nucleares, en particular el posicionamiento previo de armas nucleares, sus sistemas vectores y otras instalaciones militares estratégicas. Se deben tomar medidas integrales para evitar confrontaciones militares directas entre estados con armas nucleares, con énfasis en eliminar las causas profundas de los conflictos de seguridad.

China y la Federación de Rusia apoyan el éxito del proceso de revisión del Tratado sobre la no proliferación de las armas nucleares y, al mismo tiempo, se oponen a los intentos de utilizar el Tratado sobre la no proliferación de las armas nucleares y su proceso de revisión para la no proliferación de las armas nucleares. - Fines políticos relacionados con el contenido del Tratado.

Las partes reiteran su seria preocupación por los intentos de los Estados Unidos de socavar la estabilidad estratégica para mantener su superioridad militar absoluta, incluida, entre otras cosas, la construcción de un sistema global de defensa antimisiles por parte de los Estados Unidos y el despliegue de dichos sistemas en todo el mundo. y en el espacio, fortaleciendo la capacidad de las armas no nucleares de alta precisión para neutralizar las operaciones militares del otro lado y la capacidad de llevar a cabo ataques de decapitación, y fortaleciendo la capacidad de “compartir armas nucleares” de la Organización del Trata-

do del Atlántico Norte en Europa. La Organización del Tratado del Atlántico Norte (OTAN) también está desarrollando acuerdos de "compartición nuclear" en Europa y brindando "disuasión extendida" a aliados individuales mediante la construcción de infraestructura en Australia, parte del Tratado sobre la Zona Libre de Armas Nucleares del Pacífico Sur, que podría usarse proteger las operaciones de las fuerzas nucleares estadounidenses y británicas, desarrollar la cooperación entre submarinos nucleares estadounidenses, británicos y australianos e implementar un sistema para desplegar y proporcionar acceso a Asia-Pacífico y desde Europa. Rusia tiene planes de desplegar y suministrar a sus aliados misiles terrestres de corto y mediano alcance.

Ambas partes expresan seria preocupación porque Estados Unidos ha comenzado a tomar medidas para desplegar sistemas terrestres de misiles de alcance intermedio en la región de Asia y el Pacífico con el pretexto de realizar ejercicios conjuntos con sus aliados que claramente apuntan a China y Rusia. Estados Unidos también afirma que seguirá llevando a cabo la práctica mencionada anteriormente, con el objetivo final de hacer realidad su intención de desplegar periódicamente misiles en todo el mundo. Las dos partes condenan en los términos más enérgicos posibles estas acciones extremadamente desestabilizadoras, que representan una amenaza directa a la seguridad de China y la Federación de Rusia, y fortalecerán su coordinación y cooperación para hacer frente a la política hostil y poco constructiva de "doble contención" del conflicto. Estados Unidos unidos hacia China y la Federación Rusa.

Las partes reafirman que la Convención sobre Armas Biológicas debe cumplirse plenamente y fortalecerse e institucionalizarse continuamente con un protocolo jurídicamente vinculante que contenga un mecanismo de verificación eficaz. Las dos partes exigen que Estados Unidos se abstenga de participar en cualquier actividad biomilitar dentro o fuera de su territorio que amenace la seguridad de otros países y de la región en cuestión.

Las Partes se oponen a los intentos de Estados individuales de utilizar el espacio ultraterrestre para enfrentamientos armados, así como a las políticas y actividades de seguridad encaminadas a lograr la superioridad militar y definir y utilizar el espacio ultraterrestre como una "frontera operativa". Las partes son partidarias de iniciar lo antes posible negociaciones sobre un instrumento multilateral jurídicamente vinculante basado en el proyecto de Tratado ruso-chino sobre la prevención de la colocación de armas en el espacio ultraterrestre y de la amenaza o el uso de la fuerza contra objetos en el espacio ultraterrestre. , a fin de proporcionar garantías fundamentales y fiables para la prevención de una carrera de armamentos en el espacio ultraterrestre, la militarización del espacio ultraterrestre y el uso o la amenaza de la fuerza contra objetos espaciales o con su ayuda. Para mantener la paz mundial, garantizar la seguridad igual e indivisible de todos los Estados y mejorar la previsibilidad y sostenibilidad de la exploración y el uso pacífico del espacio ultraterrestre por todos los Estados, las dos partes respaldaron la iniciativa internacional/compromiso político de buscar globalmente la iniciativa de no desplegar armas por primera vez en el espacio ultraterrestre.

Ambas partes están comprometidas con el objetivo de un mundo libre de armas químicas y están profundamente preocupadas por la politización de la Organización para la Prohibición de las Armas Químicas (OPAQ). Las dos partes señalaron que se debe cumplir plenamente la Convención sobre la Prohibición de Armas Químicas, como mecanismo

importante en el campo del desarme y la no proliferación. Las dos partes instan a Japón a implementar de manera plena, completa y precisa el "Plan para la destrucción de armas químicas japonesas abandonadas en la República Popular China después de 2022" y a destruir las armas químicas abandonadas en China lo antes posible.

Las dos partes seguirán coordinando sus acciones sobre la cuestión del desarme y la no proliferación de armas químicas y están comprometidas a restaurar la autoridad de la Organización para la Prohibición de las Armas Químicas (OPAQ) y promover el regreso de su trabajo a un nivel más alto. técnico y no politizado.

Las dos partes reafirman su adhesión a las obligaciones de control de las exportaciones establecidas en el Tratado sobre la no proliferación de las armas nucleares, la Convención sobre la Prohibición de las Armas Biológicas y la Convención sobre la Prohibición de las Armas Químicas y se oponen a la sustitución del original no -la intención de proliferación con un propósito político hipócrita, la politización y militarización de los controles de exportación de no proliferación, el servicio de intereses nacionales miopes y la imposición de medidas restrictivas unilaterales ilegales.

Las partes reafirman su compromiso con la implementación plena y efectiva de la resolución de la Asamblea General sobre la promoción de la cooperación internacional en el uso pacífico de la seguridad internacional.

Las dos partes están dispuestas a profundizar su cooperación en la lucha contra el terrorismo y el extremismo internacional y adoptar una actitud de "tolerancia cero" hacia las "tres fuerzas", incluido el Movimiento Islámico Oriental; al mismo tiempo, están dispuestos a fortalecer aún más su cooperación en la lucha contra el crimen organizado transnacional, el extremismo y el terrorismo. Al mismo tiempo, las dos partes están dispuestas a fortalecer aún más la cooperación en la lucha contra el crimen organizado transnacional, la corrupción y el tráfico ilícito de drogas, sustancias psicotrópicas y sus precursores, y enfrentar conjuntamente otros nuevos desafíos y amenazas.

Las dos partes conceden gran importancia a la cuestión de la inteligencia artificial y están dispuestas a fortalecer los intercambios y la cooperación en su desarrollo, seguridad y gobernanza. La parte rusa da la bienvenida a la iniciativa de China sobre la Gobernanza Global de la Inteligencia Artificial, y la parte china da la bienvenida a la propuesta de la parte rusa sobre directrices de gobernanza en el campo de la inteligencia artificial. Las dos partes acordaron establecer y hacer un buen uso de un mecanismo de consulta regular para fortalecer la cooperación en IA y tecnologías de código abierto, coordinar sus posiciones al considerar cuestiones regulatorias de IA en plataformas internacionales y apoyar conferencias internacionales relacionadas con la IA organizadas por la otra parte.

Las dos partes reafirmaron su posición unánime sobre el mantenimiento de la seguridad en el campo de las tecnologías de la información y las comunicaciones y acordaron trabajar juntas para abordar varios tipos de riesgos de ciberseguridad, incluidos los relacionados con la inteligencia artificial. Las dos partes alientan al mundo a promover conjuntamente el desarrollo saludable de la IA, compartir los dividendos de la IA, fortalecer la cooperación internacional en el desarrollo de capacidades de IA, abordar adecuadamente la cuestión de las aplicaciones militares de la IA y apoyar los intercambios y la cooperación en IA dentro de las naciones. Unión Internacional de Telecomunicaciones, BRICS, Organización

de Cooperación de Shanghai, Organización Internacional de Normalización y otras plataformas de mecanismos. Se oponen al uso de monopolios tecnológicos y medidas coercitivas unilaterales para obstruir maliciosamente el desarrollo de la IA en otros países y bloquear la cadena de suministro global de la IA.

Las dos partes reconocen el papel de liderazgo de las Naciones Unidas en la formulación de reglas comunes en el campo de la seguridad de la información internacional y apoyan al Grupo de Trabajo Abierto de las Naciones Unidas sobre Seguridad de la Información 2021-2025 como una plataforma de negociación global insustituible en este campo y su trabajo habitual. Las Partes señalan que se debe desarrollar un nuevo código de conducta responsable para los Estados en el espacio de la información y, en particular, que el desarrollo de un instrumento jurídico universal podría sentar las bases para el establecimiento de un mecanismo de mediación legal internacional en el espacio de la información. información con el objetivo de prevenir conflictos entre Estados, lo que conduciría al establecimiento de un entorno de tecnología de la información y las comunicaciones pacífico, abierto, seguro, estable, interoperable y accesible. Las Partes creen que se debe implementar la resolución 74/247 de la Asamblea General de las Naciones Unidas y que se debe finalizar el desarrollo de una convención internacional integral contra el uso de tecnologías de la información y las comunicaciones con fines delictivos en el Comité Ad Hoc de las Naciones Unidas.

Las Partes apoyan la construcción de un sistema multilateral, democrático y transparente de gobernanza global de Internet basado en la premisa de garantizar la seguridad y estabilidad de los sistemas cibernéticos nacionales.

Las dos partes están dispuestas a fortalecer la colaboración en el marco de la Organización de Cooperación de Shanghai, los BRICS y otros mecanismos multilaterales. Las autoridades competentes de ambas partes están dispuestas a profundizar la cooperación bilateral en el ámbito de la seguridad de la información internacional en el marco de las leyes y tratados vigentes.

VIII

Ambas partes tomaron medidas para abordar el cambio climático y reafirmaron su compromiso con los objetivos, principios y marco institucional de la Convención Marco de las Naciones Unidas sobre el Cambio Climático y su Acuerdo de París, en particular el principio de responsabilidades comunes pero diferenciadas. Las Partes enfatizan que el apoyo financiero proporcionado por los países desarrollados a los países en desarrollo es esencial para mitigar el aumento de las temperaturas promedio globales y adaptarse a los impactos negativos del cambio climático global. Ambas partes se oponen a la creación de barreras comerciales y a la vinculación de las cuestiones climáticas con amenazas a la paz y la seguridad internacionales con el argumento de abordar el cambio climático.

Las dos partes aprecian el Marco Mundial de Biodiversidad Kunming-Montreal adoptado en la 15ª reunión de la Conferencia de las Partes en el Convenio de las Naciones Unidas sobre la Diversidad Biológica (CDB), que fue auspiciada por China, y están dispuestas a promover el desarrollo armonioso de los seres humanos. los seres humanos y la naturaleza y contribuir al desarrollo sostenible global.

Las dos partes están decididas a intensificar sus esfuerzos para combatir la contaminación por desechos plásticos basándose en el respeto de las condiciones nacionales y la soberanía de cada país, y a trabajar con todas las partes para formular un instrumento jurídicamente vinculante para abordar la contaminación ambiental (incluida la contaminación marina) causada por el plástico. desperdiciar.

Las dos partes expresan su seria preocupación por la eliminación por parte de Japón del agua contaminada de Fukushima en el océano y exigen que Japón elimine de manera segura y responsable el agua contaminada de Fukushima, se someta a una estricta vigilancia internacional y respete la solicitud de los países involucrados de llevar a cabo una vigilancia independiente.

IX

La Federación de Rusia valora positivamente la posición objetiva e imparcial de China hacia Ucrania y comparte la opinión de que la crisis debe resolverse sobre la base del pleno y completo respeto de la Carta de las Naciones Unidas.

La Federación de Rusia acoge con satisfacción la voluntad de China de desempeñar un papel constructivo en la solución política y diplomática de la crisis en Ucrania.

Las partes señalan la importancia de detener todas las acciones que contribuyan a prolongar los combates y agravar el conflicto, y piden que se evite que la crisis se salga de control. Las partes subrayan que el diálogo es una buena manera de resolver la crisis en Ucrania.

Las partes creen que para lograr una solución estable a la crisis en Ucrania, es necesario abordar las causas profundas de la crisis, adherirse al principio de indivisibilidad de la seguridad y tener en cuenta los intereses y preocupaciones legítimos de seguridad de todos los Estados.

X

Las Partes creen que los destinos de todos los pueblos son comunes y que ningún país debe buscar su propia seguridad a expensas de la seguridad de los demás. Las Partes expresan su preocupación por los desafíos de las realidades de seguridad internacional y regional y señalan que, en el contexto geopolítico actual, es necesario explorar el establecimiento de un sistema de seguridad sostenible en el espacio euroasiático basado en el principio de seguridad igual e indivisible.

Las Partes piden a los Estados y organizaciones en cuestión que dejen de adoptar políticas de confrontación e interferir en los asuntos internos de otros Estados, socavando la arquitectura de seguridad existente, construyendo “pequeños complejos y altos muros” entre los Estados, provocando tensiones en la región y defendiendo la enfrentamiento entre los bandos.

Ambos bandos se oponen a la formación de bloques cerrados y excluyentes en Asia y el Pacífico, especialmente alianzas militares contra terceros. Las dos partes señalaron que la Estrategia Indo-Pacífico de Estados Unidos y las medidas destructivas de la OTAN en la

región de Asia y el Pacífico tienen un impacto negativo sobre la paz y la estabilidad en la región.

Las dos partes expresaron su seria preocupación por las consecuencias de la Asociación Trilateral de Seguridad entre Estados Unidos, el Reino Unido y Australia (AUKUS) en diversas áreas para la estabilidad estratégica en la región de Asia y el Pacífico.

Las partes fortalecerán la coordinación para profundizar la cooperación con la ASEAN y continuarán trabajando juntas para promover la consolidación de la posición central de la ASEAN en la arquitectura multilateral de la región de Asia y el Pacífico y mejorar la eficacia de los mecanismos liderados por la ASEAN, como la Cumbre de Asia Oriental. y el Foro Regional de la ASEAN.

La Federación de Rusia apoya los esfuerzos conjuntos de China y los países de la ASEAN para mantener la paz y la estabilidad en el Mar de China Meridional. Las dos partes creen que los problemas en el Mar Meridional de China deben resolverse mediante negociaciones y consultas entre los países directamente involucrados y se oponen firmemente a la intervención de fuerzas extraterritoriales en el Mar Meridional de China. La Federación de Rusia apoya a China y a los países de la ASEAN en la implementación plena y efectiva de la Declaración sobre la Conducta de las Partes en el Mar Meridional de China y acoge con satisfacción la pronta conclusión del Código de Conducta en el Mar Meridional de China.

Ambas partes se oponen a las medidas hegemónicas de Estados Unidos para cambiar el equilibrio de poder en el noreste de Asia mediante la expansión de su poder militar y la formación de bloques militares. Estados Unidos adhiere a la mentalidad de la Guerra Fría y al modelo de confrontación de campo, y coloca la seguridad de un "pequeño grupo" por encima de la seguridad y estabilidad de la región, poniendo en riesgo la seguridad de todos los países de la región. Estados Unidos debe detener estos actos.

Las dos partes se oponen a los actos de disuasión de Estados Unidos y sus aliados en el ámbito militar, provocando un enfrentamiento con la República Popular Democrática de Corea y un posible conflicto armado, que empeoraría la tensión en la península de Corea. Las dos partes instan a Estados Unidos a tomar medidas efectivas para aliviar las tensiones militares y crear condiciones favorables, abandonar la intimidación, las sanciones y la represión, y presionar a la República Popular Democrática de Corea y a otros países involucrados para que reinicien el proceso de negociación basado en el principio de respeto mutuo y tener en cuenta las preocupaciones de cada uno en materia de seguridad. Las partes reafirman que los medios políticos y diplomáticos son la única salida a todos los problemas en la península y piden a la comunidad internacional que apoye la iniciativa conjunta constructiva de China y la Federación de Rusia.

Las partes defienden el mantenimiento de la paz y la estabilidad en Oriente Medio y se oponen a la injerencia en los asuntos internos de los estados regionales. Las partes apoyan una solución integral, justa y duradera a la cuestión de Palestina basada en el derecho internacional universalmente reconocido, con la solución de dos Estados como elemento fundamental, y esperan ver el establecimiento de un Estado de Palestina independiente basado en las fronteras de 1967. , con Jerusalén Este como su capital, viviendo en paz y seguridad junto a Israel.

Las partes apoyan la soberanía, la independencia, la unidad y la integridad territorial de los Estados de Siria y Libia y promueven un proceso de solución política dirigido y propiedad de los propios pueblos de los dos Estados.

Las dos partes cooperarán activamente para consolidar la seguridad en la región del Golfo y promover la confianza mutua y el desarrollo sostenible entre los países de la región.

Las dos partes están dispuestas a fortalecer la cooperación en asuntos afganos a nivel bilateral y bajo mecanismos multilaterales para promover a Afganistán como un país independiente, neutral, unido y pacífico, libre de terrorismo y narcóticos y que vive en armonía con todos sus vecinos. Las dos partes conceden gran importancia y apoyan el papel activo y positivo desempeñado por plataformas regionales como las reuniones de Ministros de Asuntos Exteriores de los vecinos de Afganistán, las consultas modelo de Moscú sobre Afganistán, el Mecanismo Cuadrilátero China-Rusia-Pakistán-Irán, la Cooperación de Shanghai Organización y otras plataformas regionales, en la solución política de la cuestión afgana. Ambas partes enfatizan que Estados Unidos y la OTAN han desempeñado un papel positivo y constructivo en la solución política de la cuestión afgana.

Las partes subrayan que los Estados Unidos de América y la OTAN, como partes responsables de los 20 años de agresión y ocupación de Afganistán, no deberían intentar desplegar una vez más instalaciones militares en Afganistán y la región circundante, sino que deberían asumir la responsabilidad principal por la actual dificultades económicas y sociales en Afganistán, asumir la carga de los gastos de reconstrucción del país y tomar todas las medidas necesarias para descongelar los activos del Estado afgano.

Las partes creen que la Organización del Tratado de Seguridad Colectiva y la Comunidad de Estados Independientes desempeñan un papel importante en el mantenimiento de la estabilidad regional y la lucha contra los desafíos del terrorismo internacional, la producción y el tráfico de drogas ilícitas y otras amenazas transfronterizas, como el crimen organizado. Las partes enfatizan el potencial de cooperación entre China y la Organización del Tratado de Seguridad Colectiva en áreas como el mantenimiento de la paz y la seguridad en la región euroasiática y el enfrentamiento conjunto de los desafíos externos.

Para desarrollar relaciones amistosas, estables y prósperas con los países vecinos, las partes continuarán trabajando con los países de la región de Asia Central para desarrollar una cooperación mutuamente beneficiosa y fortalecer la colaboración en organizaciones internacionales y mecanismos multilaterales como la Organización para la Cooperación de Shanghai, la Conferencia sobre Interacción y Medidas de Fomento de la Confianza en Asia y las Naciones Unidas.

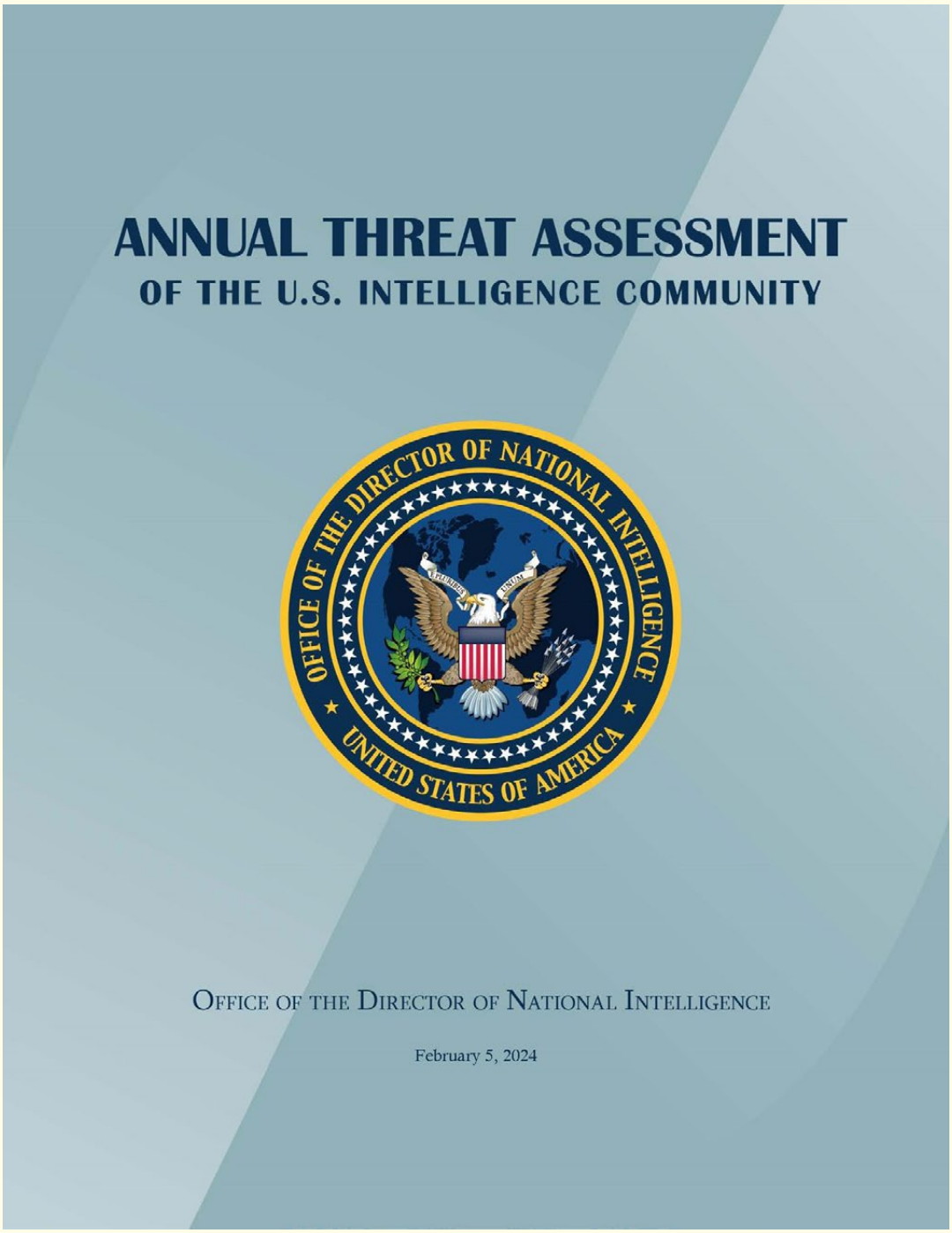
Las partes coinciden en que la paz, la estabilidad y el logro de una independencia y autonomía genuinas por parte de los Estados africanos son la base para el desarrollo y la prosperidad del continente. Las dos partes piden mantener una atmósfera sólida y saludable para la cooperación internacional con África y, con este fin, continuarán fortaleciendo su comunicación y colaboración en asuntos africanos y contribuirán a apoyar a los países africanos en la solución de los problemas africanos de una manera africana.

Las dos partes continuarán fortaleciendo la cooperación estratégica en temas de América Latina y el Caribe. Las dos partes desean fortalecer la cooperación en diversos

campos con países y mecanismos relevantes en América Latina y el Caribe, incluidos, entre otros, la Comunidad de Estados Latinoamericanos y Caribeños (CELAC), el Mercado Común del Sur (MERCOSUR), la Alianza del Pacífico. (AP), la Comunidad Andina (CAN), la Alianza Bolivariana para las Américas (ALBA), el Sistema de la Integración Centroamericana (SICA), la Comunidad del Caribe (CARICOM) y otras organizaciones. (SICA), la Comunidad del Caribe (CARICOM) y otras organizaciones regionales, así como organizaciones internacionales como las Naciones Unidas, el Grupo de los Veinte (G20) y los BRICS.

Las Partes sostienen que el Ártico debe seguir siendo un lugar de paz, estabilidad, diálogo constructivo y cooperación mutuamente beneficiosa, y que no debe crear tensiones militares y políticas en la región.

17/mayo/2024


ANNUAL THREAT ASSESSMENT
OF THE U.S. INTELLIGENCE COMMUNITY
OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
UNITED STATES OF AMERICA
OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
February 5, 2024

ANNUAL THREAT ASSESSMENT OF THE U.S. INTELLIGENCE COMMUNITY

February 5, 2024

INTRODUCTION

This annual report of worldwide threats to the national security of the United States responds to Section 617 of the FY21 *Intelligence Authorization Act* (Pub. L. No. 116-260). This report reflects the collective insights of the Intelligence Community (IC), which is committed every day to providing the nuanced, independent, and unvarnished intelligence that policymakers, warfighters, and domestic law enforcement personnel need to protect American lives and America's interests anywhere in the world.

This assessment focuses on the most direct, serious threats to the United States primarily during the next year. The order of the topics presented in this assessment does not necessarily indicate their relative importance or the magnitude of the threats in the view of the IC. All require a robust intelligence response, including those where a near-term focus may help head off greater threats in the future.

Information available as of 22 January was used in the preparation of this assessment.

[3]

CONTENTS

INTRODUCTION 3
FOREWORD 5
STATE ACTORS 7
China 7
Russia 14
Iran 18
North Korea 21
Conflicts and Fragility 24
Gaza Conflict 24
Potential Interstate Conflict 25
Potential Intrastate Turmoil 27
TRANSNATIONAL ISSUES 30
Contested Spaces 30
Disruptive Technology 30
Digital Authoritarianism and Transnational Repression 31
WMD 31
Shared Domains 33
Environmental Change and Extreme Weather 33
Health Security 33
Migration 35
Non-State Actor Issues 36
Transnational Organized Crime 36
Human Trafficking 37
Global Terrorism 38
Private Military and Security Companies 40

FOREWORD

During the next year, the United States faces an increasingly fragile global order strained by accelerating strategic competition among major powers, more intense and unpredictable transnational challenges, and multiple regional conflicts with far-reaching implications. An ambitious but anxious China, a confrontational Russia, some regional powers, such as Iran, and more capable non-state actors are challenging longstanding rules of the international system as well as U.S. primacy within it. Simultaneously, new technologies, fragilities in the public health sector, and environmental changes are more frequent, often have global impact and are harder to forecast. One need only look at the Gaza crisis—triggered by a highly capable non-state terrorist group in HAMAS, fueled in part by a regionally ambitious Iran, and exacerbated by narratives encouraged by China and Russia to undermine the United States on the global stage—to see how a regional crisis can have widespread spillover effects and complicate international cooperation on other pressing issues. The world that emerges from this tumultuous period will be shaped by whoever offers the most persuasive arguments for how the world should be governed, how societies should be organized, and which systems are most effective at advancing economic growth and providing benefits for more people, and by the powers—both state and non-state—that are most able and willing to act on solutions to transnational issues and regional crises.

New opportunities for collective action, with state and non-state actors alike, will emerge out of these complex and interdependent issues. The 2024 Annual Threat Assessment highlights some of those connections as it provides the IC's baseline assessments of the most pressing threats to U.S. national interests. It is not an exhaustive assessment of all global challenges, however. It addresses traditional and nontraditional threats from U.S. adversaries, an array of regional issues with possible larger, global implications, as well as functional and transnational challenges, such as proliferation, emerging technology, climate change, terrorism, and illicit drugs.

China has the capability to directly compete with the United States and U.S. allies and to alter the rules-based global order in ways that support Beijing's power and form of governance over that of the United States. China's serious demographic and economic challenges may make it an even more aggressive and unpredictable global actor. Russia's ongoing aggression in Ukraine underscores that it remains a threat to the rules-based international order. Local and regional powers are also trying to gain and exert influence, often at the cost of neighbors and the world order itself. Iran will remain a regional menace with broader malign influence activities, and North Korea will expand its WMD capabilities while being a disruptive player on the regional and world stages. Often, U.S. actions intended to deter foreign aggression or escalation are interpreted by adversaries as reinforcing their own perceptions that the United States is intending to contain or weaken them, and these misinterpretations can complicate escalation management and crisis communications.

Regional and localized conflicts and instability, such as from the HAMAS attacks against Israel and Israel's subsequent invasion of Gaza, will demand U.S. attention as states and non-state actors struggle in this evolving global order, including over major power competition and shared transnational challenges. From this, conflicts and bouts of instability from East Asia to Africa to the Western Hemisphere—exacerbated by global challenges—have greater potential to spill over into many domains, with implications for the United States, U.S. allies and partners, and the world.

Economic strain is further stoking this instability. Around the world, multiple states are facing rising, and in some cases unsustainable, debt burdens, economic spillovers from the war in Ukraine, and increased cost and output losses from extreme weather events even as they continue to recover from the COVID-19 pandemic. While global agricultural food commodity prices retreated from their 2022 peak, domestic food price inflation remains high in many countries and food security in many countries remains vulnerable to economic and geopolitical shocks.

At the same time, the world is beset by an array of shared, universal issues requiring cooperative global solutions. However, the larger competition between democratic and authoritarian forms of government that China, Russia, and other countries are fueling by promoting authoritarianism and spreading disinformation is putting pressure on longstanding norms encouraging cooperative approaches to the global commons. This competition also exploits technological advancements—such as AI, biotechnologies and related biosecurity, the development and production of microelectronics, and potential quantum developments—to gain stronger sway over worldwide narratives affecting the global geopolitical balance, including influence within it. The fields of AI and biotechnology, in particular, are rapidly advancing, and convergences among various fields of science and technology probably will result in further significant breakthroughs. The accelerating effects of climate change are placing more of the world's population, particularly in low- and middle-income countries, at greater risk from extreme weather, food and water insecurity, and humanitarian disasters, fueling migration flows and increasing the risks of future pandemics as pathogens exploit the changing environment.

The 2024 Annual Threat Assessment report supports the Office of the Director of National Intelligence's commitment to transparency and the tradition of providing regular threat updates to the American public and the United States Congress. The IC is vigilant in monitoring and assessing direct and indirect threats to U.S. and allied interests. For this requirement, the IC's National Intelligence Officers—and the National Intelligence Council that they collectively constitute—work closely and regularly with analysts across the IC. This work diagnostically examines the most serious of both the immediate and long-term threats to the United States, along with the evolving global order and other macro-trends, that will most influence the direction and potential impact of these threats.

The National Intelligence Council stands ready to support policymakers with additional information in a classified setting.

[6]

STATE ACTORS

PREFACE

Several states are engaging in competitive behavior that directly threatens U.S. national security while a larger set of states—including some allies—are facing intrastate conflict or domestic turmoil. These pressures and dynamics have the potential to spill over borders and across regions to destabilize areas and threaten the livelihoods, safety, and stability of billions of people. China vies to surpass the United States in comprehensive national power and secure deference to its preferences from its neighbors and from countries around the world, while Russia directly threatens the United States in an attempt to assert leverage regionally and globally.

CHINA

Regional and Global Activities

President Xi Jinping envisions China as the preeminent power in East Asia and as a leading power on the world stage. The Chinese Communist Party (CCP) will attempt to preempt challenges to its reputation and legitimacy, undercutting U.S. influence, driving wedges between Washington and its partners, and fostering global norms that favor its authoritarian system. Most significantly, the People's Republic of China (PRC) will press Taiwan on unification, an effort that will create critical friction points with the United States. Despite economic setbacks, China's leaders will maintain statist economic policies to steer capital toward priority sectors, reduce dependence on foreign technologies, and enable military modernization.

- China views Washington's competitive measures against Beijing as part of a broader U.S. diplomatic, economic, military, and technological effort to contain its rise, undermine CCP rule, and prevent the PRC from achieving its regional and global power ambitions. Nevertheless, China's leaders will seek opportunities to reduce tension with Washington when they believe it benefits Beijing and protects core interests, such as Xi's willingness to meet with President Biden at the APEC Summit in late 2023.

- China faces myriad domestic challenges that probably will hinder CCP leaders' ambitions. CCP leaders have long believed that China's technology-powered economic growth would outpace Western countries. However, China's growth almost certainly will continue slowing thanks to demographic challenges and a collapse in consumer and investor sentiment due in large part to Beijing's heavyhanded policies.

- PRC leaders' regional and global ambitions are also hampered by growing resistance to China's heavyhanded and coercive economic, diplomatic, and military tactics toward Taiwan and other countries. In particular, China's policies have led many countries and businesses to accelerate de-risking in key sectors and to limit exports of sensitive technology to China, which is further hindering PRC leaders' goals for technology-enabled economic and military development.

The PRC combines its economic heft with its growing military power and its diplomatic and technological dominance for a coordinated approach to strengthen CCP rule, secure what it views as its sovereign territory and regional preeminence, and pursue global power. In particular, Beijing uses these whole-of-government tools to compel others to acquiesce to its preferences, including its assertions of sovereignty over Taiwan.

- In 2024, following Taiwan's presidential and legislative election, Beijing will continue to apply military and economic pressure as well as public messaging and influence activities while promoting long-term cross-Strait economic and social integration to induce Taiwan to move toward unification. Taiwan is a significant potential flashpoint for confrontation between the PRC and the United States as Beijing claims that the United States is using Taiwan to undermine China's rise. Beijing will use even stronger measures to push back against perceived increases in U.S. support to Taiwan.

- In the South China Sea, Beijing will continue to use its growing military and other maritime capabilities to try to intimidate rival claimants and to signal it has control over contested areas. Similarly, China is pressing Japan over contested areas in the East China Sea.

- Beijing aims to expand its influence abroad and be viewed as a champion of global development via several multinational forums and PRC-branded initiatives such as the Belt and Road Initiative, the Global Development Initiative, and the Global Security Initiative. China is promoting an alternative to existing, often Western-dominated international development and security forums in favor of norms that support state sovereignty and place political stability over individual rights. As part of this effort, Beijing seeks to champion development and security in the Global South—areas that Beijing perceives are receptive to engagement with China because of shared historical experiences under colonial and imperialistic oppression—as a way to build global influence; demonstrate leadership; and expand its economic, diplomatic, and military presence.

Beijing is balancing the level of its support to Moscow to maintain the relationship without incurring risk to its own economic and diplomatic interests. In return, China is securing favorable energy prices and greater access to the Arctic.

- The PRC is providing economic and security assistance to Russia's war in Ukraine through support to Russia's defense industrial base, including by providing dual-use material and components for weapons. Trade between China and Russia has been increasing since the start of the war in Ukraine, and PRC exports of goods with potential military use rose more than threefold since 2022.

Economics

During the next few years, China's economy will slow because of structural barriers and Beijing's unwillingness to take aggressive stimulus measures to boost economic growth. Beijing understands its problem but is avoiding reforms at odds with Xi's prioritization of state-directed investment in manufacturing and industry. A slower Chinese economy probably would depress commodity prices

worldwide, erode export competitiveness of countries that directly compete against China, and slow global growth, but it is unlikely to curtail Beijing's spending on state priorities.

- China's slowing economy could create resource constraints in the long run and force it to prioritize spending between social issues, industrial policy, military, and overseas lending.
- Xi is prioritizing what he deems "high-quality growth"—which includes greater self-sufficiency in strategic sectors and a more equitable distribution of wealth—replacing the focus on maximizing GDP growth, while also attempting to mitigate the threat of U.S. sanctions and unhappiness with semiconductor export controls.

Technology

China seeks to become a world S&T superpower and to use this technological superiority for economic, political, and military gain. Beijing is implementing a whole-of-government effort to boost indigenous innovation and promote self-reliance, and is prioritizing advanced power and energy, AI, biotechnology, quantum information science, and semiconductors. Beijing is trying to fast-track its S&T development through investments, intellectual property (IP) acquisition and theft, cyber operations, talent recruitment, scientific and academic collaboration, and illicit procurements.

- In 2023, a key PRC state-owned enterprise has signaled its intention to channel at least $13.7 billion into emerging industries such as AI, advanced semiconductors, biotechnology, and new materials. China also announced its Global AI Governance Initiative to bolster international support for its vision of AI governance.
- China now rivals the United States in DNA-sequencing equipment and some foundational research. Beijing's large volume of genetic data potentially positions it to lead in precision medicine and agricultural biotechnology applications.
- China is making progress in producing advanced chips for cryptocurrency mining and cellular devices at the 7-nanometer (nm) level using existing equipment but will face challenges achieving high-quality, high-volume production of cutting-edge chips without access to extreme ultraviolet lithography tools. By 2025, 40 percent of all 28-nm legacy chips are projected to be produced in China, judging from the number of new factories expected to begin operating during the next two years.

WMD

China remains intent on orienting its nuclear posture for strategic rivalry with the United States because its leaders have concluded their current capabilities are insufficient. Beijing worries that bilateral tension, U.S. nuclear modernization, and the People's Liberation Army's (PLA) advancing conventional capabilities have increased the likelihood of a U.S. first strike. As its nuclear force grows, Beijing's confidence in its nuclear deterrent probably will bolster the PRC's resolve and intensify conventional conflicts.

- China probably has completed construction of more than 300 new ICBM silos and has loaded at least some of those silos with missiles.

China probably possesses capabilities relevant to chemical and biological warfare (CBW) that pose a threat to U.S., allied, and partner forces as well as civilian populations.

Military

Beijing will focus on building a fully modernized national defense and military force by 2035 and for the PLA to become a world-class military by 2049. In the meantime, the CCP hopes to use the PLA to secure what it claims is its sovereign territory, to assert its preeminence in regional affairs, and to project power globally, particularly by being able to deter and counter an intervention by the United States in a cross-Strait conflict. However, China lacks recent warfighting experience, which probably would weaken the PLA's effectiveness and leaders' willingness to initiate a conflict. In addition, PRC leaders almost certainly are concerned about the ongoing impact of corruption on the military's capabilities and reliability, judging from a purge of high-level officers including the defense minister in 2023.

- The PLA has fielded modern systems and improved its competency to conduct joint operations that will threaten U.S. and allied forces in the western Pacific. It operates two aircraft carriers and is expected to commission its most advanced carrier in 2024, operates a host of ballistic and cruise missiles as well as the DF-17 hypersonic glide vehicle, and is fielding fifth-generation fighter aircraft.

- PLA ground forces have conducted increasingly realistic training scenarios to improve their readiness and ability to execute operations, including a potential cross-Strait invasion.

The PLA is developing and deploying new technologies to enhance its capability to process and use information at scale and machine speed, allowing decisionmakers to plan, operate, and support cross-domain unconventional and asymmetrical fighting. The PLA is researching various applications for AI, including support for missile guidance, target detection and identification, and autonomous systems.

- The PLA is accelerating the incorporation of command information systems, providing forces and commanders with enhanced situational awareness and decision support to more effectively carry out joint missions and tasks.

The PLA will continue to pursue the establishment of overseas military installations and access agreements in an attempt to project power and protect China's interests abroad. Beyond developing its military base in Djibouti and its military facility at Ream Naval Base in Cambodia, Beijing reportedly is considering pursuing military facilities in multiple locations, including—but not limited to—Burma, Cuba, Equatorial Guinea, Pakistan, Seychelles, Sri Lanka, Tajikistan, Tanzania, and the UAE.

For at least a decade, Beijing and Moscow have used high-profile, combined military activities to signal the strength of the China–Russia defense relationship but have made only minor enhancements to interoperability in successive exercises.

Space

China remains committed to becoming a world-class space leader and continues to demonstrate its growing prowess by deploying increasingly capable space systems and working towards ambitious scientific feats. By 2030, China probably will achieve world-class status in all but a few space technology areas.

- Space-based intelligence, surveillance, and reconnaissance (ISR), as well as position, navigation, and timing, and satellite communications are areas the PLA continues to improve upon to close the perceived gap between itself and the U.S. military.
- In early 2023, China's Manned Space Agency announced its intention to land astronauts on the Moon around 2030 and is engaging countries to join its lunar research station effort as part of its broader attempt to develop an alternative bloc to the U.S.-led Artemis Accords.
- China's commercial space sector is growing quickly and is on pace to become a major global competitor by 2030. For example, China is developing its own low-earth orbit (LEO) satellite Internet service to compete with Western commercial satellite Internet services.

Counterspace operations will be integral to potential PLA military campaigns, and China has counterspace-weapons capabilities intended to target U.S. and allied satellites. China already has fielded ground-based counterspace capabilities including electronic warfare (EW) systems, directed energy weapons, and antisatellite (ASAT) missiles intended to disrupt, damage, and destroy target satellites.

- China also has conducted orbital technology demonstrations, which while not counterspace weapons tests, prove China's ability to operate future space-based counterspace weapons.

Cyber

China remains the most active and persistent cyber threat to U.S. Government, private-sector, and critical infrastructure networks. *Beijing's cyber espionage pursuits and its industry's export of surveillance, information, and communications technologies increase the threats of aggressive cyber operations against the United States and the suppression of the free flow of information in cyberspace.*

- PRC operations discovered by the U.S. private sector probably were intended to pre-position cyber attacks against infrastructure in Guam and to enable disrupting communications between the United States and Asia.
- If Beijing believed that a major conflict with the United States were imminent, it would consider aggressive cyber operations against U.S. critical infrastructure and military assets. Such a strike would be designed to deter U.S. military action by impeding U.S. decisionmaking, inducing societal panic, and interfering with the deployment of U.S. forces.
- China leads the world in applying surveillance and censorship to monitor its population and repress dissent. Beijing conducts cyber intrusions targeted to affect U.S. and non-U.S. citizens beyond its borders—including journalists, dissidents, and individuals it views as threats—to counter views it considers critical of CCP narratives, policies, and actions.

[11]

Malign Influence Operations

Beijing is expanding its global covert influence posture to better support the CCP's goals. The PRC aims to sow doubts about U.S. leadership, undermine democracy, and extend Beijing's influence. Beijing's information operations primarily focus on promoting pro-China narratives, refuting U.S.-promoted narratives, and countering U.S. and other countries' policies that threaten Beijing's interests, including China's international image, access to markets, and technological expertise.

- Beijing's growing efforts to actively exploit perceived U.S. societal divisions using its online personas move it closer to Moscow's playbook for influence operations.
- China is demonstrating a higher degree of sophistication in its influence activity, including experimenting with generative AI. TikTok accounts run by a PRC propaganda arm reportedly targeted candidates from both political parties during the U.S. midterm election cycle in 2022.
- Beijing is intensifying efforts to mold U.S. public discourse—particularly on core sovereignty issues, such as Hong Kong, Taiwan, Tibet, and Xinjiang. The PRC monitors Chinese students abroad for dissident views, mobilizes Chinese student associations to conduct activities on behalf of Beijing, and influences research by U.S. academics and think tank experts.

The PRC may attempt to influence the U.S. elections in 2024 at some level because of its desire to sideline critics of China and magnify U.S. societal divisions. PRC actors' have increased their capabilities to conduct covert influence operations and disseminate disinformation. Even if Beijing sets limits on these activities, individuals not under its direct supervision may attempt election influence activities they perceive are in line with Beijing's goals.

Intelligence Operations

China will continue to expand its global intelligence posture to advance the CCP's ambitions, challenge U.S. national security and global influence, quell perceived regime threats worldwide, and steal trade secrets and IP to bolster China's indigenous S&T sectors.

- Officials of the PRC intelligence services will try to exploit the ubiquitous technical surveillance environment in China and expand their use of monitoring, data collection, and advanced analytic capabilities against political security targets beyond China's borders. China is rapidly expanding and improving its AI and big data analytics capabilities for intelligence operations.
- More robust intelligence operations also increase the risk that these activities have international consequences, such as the overflight of the United States by the high-altitude balloon in February 2023.

Challenges

Xi Jinping's prioritization of security and stability for the CCP is undermining China's ability to solve complex domestic problems and will impede achieving the CCP's goal of becoming a major power on the world stage. China's leaders probably are most concerned about corruption, demographic

imbalances, and fiscal and economic struggles—all of which influence economic performance and quality of life, two key factors underpinning domestic support for the government and political stability.

- Beijing's growing national security focus has generated new laws on data security and anti-espionage targeting foreign firms, driven a crackdown on PRC technology companies, and calls for all of China's society to participate in counterintelligence activities.
- Xi continues to regularly reprimand, publicly warn, investigate, and conduct firings based on the dangers of corruption. However, anti-corruption efforts probably never will uproot underlying problems because of the unrivaled power of top party officials, and Xi's insistence that the party apparatus has exclusive power to monitor and fight corruption.
- Despite an easing of restrictions on birth limits, China's birth rate continues to decline. Marriage rates are on a similar downward trajectory, which will reinforce negative population trends and a shrinking labor force.
- Xi's blending of domestic and foreign security threats is undermining China's position and standing abroad, reducing Beijing's ability to influence global perceptions and achieve its objectives. Beijing's hardline approach to alleged separatism in Xinjiang, Hong Kong, and Tibet, as well as broader crackdowns on religion and dissent in China, have generated widespread global criticism of China's human rights abuses and extraterritorial interference.

RUSSIA

Regional and Global Activities

Russia's war of aggression against Ukraine has resulted in enormous damage at home and abroad, but Russia remains a resilient and capable adversary across a wide range of domains and seeks to project and defend its interests globally and to undermine the United States and the West. Russia's strengthening ties with China, Iran, and North Korea to bolster its defense production and economy are a major challenge for the West and partners. Russia will continue to pursue its interests in competitive and sometimes confrontational and provocative ways and press to influence other countries in the post–Soviet space to varying extents.

- Russia almost certainly does not want a direct military conflict with U.S. and NATO forces and will continue asymmetric activity below what it calculates to be the threshold of military conflict globally. President Vladimir Putin probably believes that Russia has blunted Ukrainian efforts to retake significant territory, that his approach to winning the war is paying off, and that Western and U.S. support to Ukraine is finite, particularly in light of the Israel–HAMAS war.

- Putin has upended Russia's geopolitical, economic, and military revival and damaged its international reputation with the large-scale invasion of Ukraine. Nevertheless, Russia is implementing policies to mitigate these costs and leveraging foreign relationships to minimize sanctions-related damage and rebuild its credibility as a great power.

- Moscow's deep economic engagement with Beijing provides Russia with a major market for its energy and commodities, greater protection from future sanctions, and a stronger partner in opposing the United States. China is by far Russia's most important trading partner with bilateral trade reaching more than $220 billion in 2023, already surpassing their record total 2022 volume by 15 percent.

Moscow will continue to employ all applicable sources of national power to advance its interests and try to undermine the United States and its allies, but it faces a number of challenges, such as severance from Western markets and technology and flight of human capital, in doing so. This will range from using energy to try to coerce cooperation and weaken Western unity on Ukraine, to military and security intimidation, malign influence, cyber operations, espionage, and subterfuge.

- Russia's GDP is on a trajectory for modest growth in 2024 but its longer-term competitiveness has diminished in comparison to its pre-war outlook. Russia has increased social spending, which probably has reduced public backlash, and increased corporate taxes, which has provided enhanced budget flexibility and financing options.

- Moscow has successfully diverted most of its seaborne oil exports and probably is selling significant volumes above the G-7–led crude oil and refined product price caps, which came into effect in December 2022 and February 2023, respectively—in part because Russia is increasing its use of non-Western options to facilitate diversion of most of its seaborne oil exports and because global oil prices increased last year.

[14]

- Russia will retain significant energy leverage. In the first half of 2023, Russia was still the second-largest supplier of liquefied natural gas to Europe and announced reduction in its crude oil exports as part of its OPEC+ commitment.

- Russia is offsetting its decline in relations with the West by expanding ties to China, Iran, North Korea, and key Global South countries.

- The renewed efforts of Armenia, Moldova, and some Central Asian states to seek alternative partners highlight how the war has hurt Moscow's influence, even in the post-Soviet space. Russia's unwillingness to expend the resources and political capital to prevent Azerbaijan from reacquiring Nagorno-Karabakh from ethnic Armenians through a military offensive in September 2023 underscores how Moscow's war in Ukraine has weakened its role as a regional security arbiter.

Conflict in Ukraine

Russia's so-called special military operation against Ukraine has incurred major, lasting costs for Russia, failed to attain the complete subjugation of Ukraine that Putin initially sought, and rallied the West to defend against Russian aggression. Russia has suffered more military losses than at any time since World War II—roughly 300,000 casualties and thousands of tanks and armored combat vehicles.

- The Russian military has and will continue to face issues of attrition, personnel shortages, and morale challenges, though its reliance on mines, prepared defensive positions, and indirect fires has helped it blunt Ukraine's offensives in 2023.

- Nonetheless, this deadlock plays to Russia's strategic military advantages and is increasingly shifting the momentum in Moscow's favor. Russia's defense industry is significantly ramping up production of a panoply of long-range strike weapons, artillery munitions, and other capabilities that will allow it to sustain a long high-intensity war if necessary. Meanwhile, Moscow has made continual incremental battlefield gains since late 2023, and is benefitting from uncertainties about the future of Western military assistance.

Military

Moscow's military forces will face a multi-year recovery after suffering extensive equipment and personnel losses during the Ukraine conflict. Moscow will be more reliant on nuclear and counterspace capabilities for strategic deterrence as it works to rebuild its ground force. Regardless, Russia's air and naval forces will continue to provide Moscow with some global power projection capabilities.

- Moscow's announced plans to massively expand its ground forces almost certainly will fall short, but nonetheless will over time result in a larger even if not qualitatively better military. Russia has been successfully recruiting record numbers of contract enlisted personnel by offering significant benefits and manipulating propaganda about the war in Ukraine. Ongoing increases in defense spending probably will provide sufficient funding to gradually increase manpower without Moscow having to resort to mobilizing reservists.

Russian Private Military and Security Companies and Paramilitary Activities

Russia will rely on private military and security companies (PMSCs) and paramilitary groups to achieve its objectives on the battlefield in Ukraine, to augment Russian forces, to move weapons and to train fighters, to hide Moscow's hand in sensitive operations, and to project influence and power in the Middle East and Africa.

WMD

Russia will continue to modernize its nuclear weapons capabilities and maintains the largest and most diverse nuclear weapons stockpile. Moscow views its nuclear capabilities as necessary for maintaining deterrence and achieving its goals in a potential conflict against the United States and NATO, and it sees this as the ultimate guarantor of the Russian Federation.

- Russia's inability to achieve quick and decisive battlefield wins, coupled with Ukrainian strikes within Russia, continues to drive concerns that Putin might use nuclear weapons. In 2023, Putin publicly touted his willingness to move nuclear weapons to Belarus in response to a longstanding request from Minsk.

- Moscow will continue to develop long-range nuclear-capable missiles and underwater delivery systems meant to penetrate or bypass U.S. missile defenses. Russia is expanding and modernizing its large and diverse set of nonstrategic systems, which are capable of delivering nuclear or conventional warheads, because Moscow believes such systems offer options to deter adversaries, control the escalation of potential hostilities, and counter U.S. and Allied conventional forces.

Russia will continue to pose a CBW threat. Scientific institutes there have researched and developed CBW capabilities, including technologies to deliver CBW agents. Russia retains an undeclared chemical weapons program and has used chemical weapons at least twice during recent years: in assassination attempts with Novichok nerve agents, also known as fourth-generation agents, against Russian opposition leader Aleksey Navalny in 2020 and against UK citizen Sergey Skripal and his daughter Yuliya Skripal on UK soil in 2018.

Cyber

Russia will pose an enduring global cyber threat even as it prioritizes cyber operations for the Ukrainian war. Moscow views cyber disruptions as a foreign policy lever to shape other countries' decisions and continuously refines and employs its espionage, influence, and attack capabilities against a variety of targets.

- Russia maintains its ability to target critical infrastructure, including underwater cables and industrial control systems, in the United States as well as in allied and partner countries.

[16]

Malign Influence Operations

Russia will remain a serious foreign influence threat because of its wide-ranging efforts to try to divide Western alliances, undermine U.S. global standing, and sow domestic discord, including among voters inside the United States and U.S. partners around the world. Russia's war in Ukraine will continue to feature heavily in its messaging.

- Moscow views U.S. elections as opportunities and has conducted influence operations for decades and as recently as the U.S. midterm elections in 2022. Russia is contemplating how U.S. electoral outcomes in 2024 could impact Western support to Ukraine and probably will attempt to affect the elections in ways that best support its interests and goals.
- Russia's influence actors have adapted their efforts to better hide their hand, and may use new technologies, such as generative AI, to improve their capabilities and reach into Western audiences.

Space

Russia will remain a key space competitor despite facing difficulties from the effects of additional international sanctions and export controls, domestic space-sector problems, and increasingly strained competition for program resources within Russia. Moscow is prioritizing assets critical to its national security and integrating space services—such as communications; positioning, navigation, and timing; and ISR.

- Moscow employs its civil and commercial remote-sensing satellites to supplement military-dedicated capabilities and has warned that other countries' commercial infrastructure in outer space used for military purposes can become a legitimate target.
- Russia continues to train its military space elements and field new antisatellite weapons to disrupt and degrade U.S. and allied space capabilities. It is expanding its arsenal of jamming systems, directed energy weapons, on-orbit counterspace capabilities, and ground-based ASAT missiles that are designed to target U.S. and allied satellites.
- Russia is investing in EW and directed energy weapons to counter Western on-orbit assets and continues to develop ground-based ASAT missiles capable of destroying space targets in LEO.

Challenges

While Putin portrays the failure of the PMSC Vagner revolt in June 2023 as evidence that Russian society is united behind his leadership, he continues to face domestic challenges, including support from elites, economic pressure, and the burden of the war in Ukraine.

- Moscow probably needs to balance increased military spending with the need for additional revenue without overburdening private and state-backed firms or the Russian public with the cost of the war. Russia faces long-term problems including a lack of foreign investment, particularly in its energy sector.

IRAN

Regional and Global Activities

Iran will continue to threaten U.S. interests, allies, and influence in the Middle East and intends to entrench its emergent status as a regional power while minimizing threats to the regime and the risk of direct military conflict. Tehran will try to leverage recent military successes through its emboldened threat network, diplomatic gains, its expanded nuclear program, and its military sales to advance its ambitions, including by trying to further bolster ties with Moscow. Iran will seek to use the Gaza conflict to denounce Israel, decry its role in the region, and try to dissuade other Middle Eastern states from warming ties with Israel, while trumpeting Iran's own role as the champion of the Palestinian cause. However, Iran's position on the conflict is unlikely to mask the challenges that it faces internally, where economic underperformance and societal grievances still test the regime.

- Decades of cultivating ties, providing support, funding, weapons, and training to its partners and proxies around the Middle East, including Lebanese Hizballah, the Huthis, and Iranian-backed militias in Iraq and Syria, will enable Tehran to continue to demonstrate the efficacy of leveraging these members of the "Axis of Resistance", a loose consortium of like-minded terrorist and militant actors. Tehran was able to flex the network's military capabilities in the aftermath of HAMAS' attack on 7 October, orchestrating anti-Israel and anti-U.S. attacks from Lebanon to the Bab al-Mandeb Strait while shielding Iranian leaders from significant consequences.

- During 2023, Iran expanded its diplomatic influence through improved ties with Russia, Saudi Arabia, and Iraq. Iran stipulated a readiness to re-implement the 2015 Joint Comprehensive Plan of Action (JCPOA) to gain sanctions relief, but Tehran's continued support to terrorist proxies and threats to former U.S. officials have not favored a deal.

- The economic, political, and societal seeds of popular discontent are still present in Iran and could threaten further domestic strife such as was seen in the wide-scale and prolonged protests inside of Iran during late 2022 and early 2023.

- Iran also will continue to directly threaten U.S. persons in the Middle East and remains committed to its decade-long effort to develop surrogate networks inside the United States. Iran seeks to target former and current U.S. officials as retaliation for the killing of Islamic Revolutionary Guard Corps (IRGC)-Qods Force Commander Qasem Soleimani in January 2020, and previously has attempted to conduct lethal operations in the United States.

- The conflict in Gaza and Iran's support to HAMAS could further weaken Iran's attempts to improve its international stature and entice foreign investment.

Iran will remain a threat to Israel and U.S. allies and interests in the region well after the Gaza conflict, and probably will continue arming and aiding its allies to threaten the United States as well as backing HAMAS and others who seek to block a peace settlement between Israel and the Palestinians. While Iran will remain careful to avoid a direct conflict with either Israel or the United States, it nonetheless enabled scores of militia rocket, missile, and UAV attacks against U.S. forces in Iraq and Syria; Hizballah exchanges of fire with Israel on the north border with Lebanon; and Huthi missile and

[18]

UAV attacks, both on Israel directly and on international commercial shipping transiting the Red Sea.

WMD

Iran is not currently undertaking the key nuclear weapons-development activities necessary to produce a testable nuclear device. Since 2020, however, Tehran has stated that it is no longer constrained by any JCPOA limits, and Iran has greatly expanded its nuclear program, reduced IAEA monitoring, and undertaken activities that better position it to produce a nuclear device, if it chooses to do so.

- Iran uses its nuclear program to build negotiating leverage and respond to perceived international pressure. Tehran said it would restore JCPOA limits if the United States fulfilled its JCPOA commitments and the IAEA closed its outstanding safeguards investigations. Tehran down blended a small quantity of 60 percent enriched uranium and significantly lowered its rate of production from June to November 2023.

- Iran continues to increase the size and enrichment level of its uranium stockpile, and develop, manufacture, and operate advanced centrifuges. Tehran has the infrastructure and experience to quickly produce weapons-grade uranium, if it chooses to do so.

- Iran probably will consider installing more advanced centrifuges, further increasing its enriched uranium stockpile, or enriching uranium up to 90 percent in response to additional sanctions, attacks, or censure against its nuclear program.

Iran probably aims to continue research and development of chemical and biological agents for offensive purposes. Iranian military scientists have researched chemicals, toxins, and bioregulators, all of which have a wide range of sedation, dissociation, and amnestic incapacitating effects.

Military

Iran's hybrid approach to warfare—using both conventional and unconventional capabilities—will pose a threat to U.S. interests in the region for the foreseeable future. Iran's unconventional warfare operations and network of militant partners and proxies enable Tehran to pursue its interests and maintain strategic depth with a modicum of deniability.

- Iran has started taking delivery of advanced trainer aircraft and probably will seek to acquire new conventional weapon systems, such as advanced fighter aircraft, helicopters, and main battle tanks. However, budgetary constraints will slow the pace and scale of acquisitions.

- Iran's missile, UAV, air defense, and naval capabilities will continue to threaten U.S. and partner commercial and military assets in the Middle East.

Iran's ballistic missile programs have the largest inventory in the region and Tehran is emphasizing improving the accuracy, lethality, and reliability of its missiles. Meanwhile, Iran's work on space launch vehicles (SLVs)—including its Simorgh—would shorten the timeline to produce an ICBM, if it decided to develop one, because the systems use similar technologies.

Cyber and Malign Influence Operations

Iran's growing expertise and willingness to conduct aggressive cyber operations make it a major threat to the security of U.S. and allied and partner networks and data. Tehran's opportunistic approach to cyber attacks puts U.S. infrastructure at risk for being targeted, particularly as its previous attacks against Israeli targets show that Iran is willing to target countries with stronger cyber capabilities than itself. Iran will continue to conduct malign influence operations in the Middle East and in other regions, including trying to undermine U.S. political processes and amplify discord.

Ahead of the U.S. election in 2024, Iran may attempt to conduct influence operations aimed at U.S. interests, including targeting U.S. elections, having demonstrated a willingness and capability to do so in the past.

- During the U.S. election cycle in 2020, Iranian cyber actors obtained or attempted to obtain U.S. voter information, sent threatening emails to voters, and disseminated disinformation about the election. The same Iranian actors have evolved their activities and developed a new set of techniques, combining cyber and influence capabilities, that Iran could deploy during the U.S. election cycle in 2024.

Challenges

Despite weathering protests in late 2022 and early 2023, Iran continues to face domestic challenges that constrain the regime's ability to achieve its goals. Mismanagement and international sanctions are brakes on the economy that limit the regime's ability to buy domestic support and legitimacy.

- Iran's economy continues to struggle amidst high inflation—likely to top 40 percent for 2023, sanctions pressure, and a depreciating currency. Most wages are unable to keep pace with the higher prices, leading to declines in households' spending power. During the coming years, Iran also will be increasingly challenged by climate change as water becomes scarcer.

- Iran's dependency on oil export revenues and slowing economic growth in China—Iran's largest buyer of oil—portend weaker revenues for Tehran and potentially higher budget deficits, probably forcing lower government spending on infrastructure, including for power and water.

- Iran's Supreme Leader, Ali Khamenei, has been serving in the position since 1989 and is in his mid-80s. His eventual passing could challenge a system characterized by elite factionalism that has only undergone a single supreme leader transition.

[20]

NORTH KOREA

Regional and Global Activities

North Korean leader Kim Jong Un will continue to pursue nuclear and conventional military capabilities that threaten the United States and its allies, which will enable periodic aggressive actions as he tries to reshape the regional security environment in his favor. North Korea has emerged from its deepest period of isolation driven by a combination of nearly two decades of severe UN sanctions and its self-imposed COVID-19 lockdown. Today, it is pursuing stronger ties with China and Russia with the goal of increasing financial gains, diplomatic support, and defense cooperation. Kim almost certainly has no intentions of negotiating away his nuclear program, which he perceives to be a guarantor of regime security and national pride. In addition, Kim probably hopes that he can use his bourgeoning defense ties with Russia to pursue his goal of achieving international acceptance as a nuclear power.

- In late 2023, Kim hosted high-level Chinese and Russian delegations in Pyongyang, and made his first trip overseas since the onset of the COVID-19 pandemic to meet with President Putin. Since this meeting, North Korea probably has begun shipping munitions to Russia in support of the conflict with Ukraine in exchange for diplomatic, economic, and military concessions.

- In response to strengthening trilateral cooperation between the United States, Japan, and South Korea, Pyongyang has sought to demonstrate the danger posed by its military through missile launches and rhetoric threatening nuclear retaliation. North Korea routinely times its missile launches and military demonstrations to counter U.S.–South Korea exercises in part to attempt to coerce both countries to change their behavior and counteract South Korean President Yoon Suk Yeol's hardline policies toward the North.

- North Korea increasingly will engage in illicit activities, including cyber theft labor deployments and the import and export of UN-proscribed commodities, to fund regime priorities such as the WMD program.

WMD

Kim remains strongly committed to expanding the country's nuclear weapons arsenal, which serves as the centerpiece of his national security structure.

- In March 2023, Kim ordered an increase in the nuclear weapons stockpile and the expansion of weapon-grade nuclear material production. North Korea also unveiled a purported tactical nuclear warhead and claimed it could be mounted on at least eight delivery systems, including an unmanned underwater vehicle and cruise missiles.

- North Korea has been prepared to resume nuclear tests at the Pungyye site since mid-2022.

North Korea maintains its CBW capabilities, and Pyongyang may use such weapons during a conflict or in an unconventional or clandestine attack.

[21]

Military

North Korea's military will pose a serious threat to the United States and its allies by its investment in niche capabilities designed to provide Kim with options to deter outside intervention, offset enduring deficiencies in the country's conventional forces, and advance his political objectives through coercion. Kim remains strongly committed to developing capabilities intended to challenge regional missile defense, diversify options to deliver nuclear warheads, and enhance second-strike capabilities.

- North Korea is working to develop its conventional capabilities, although testing and fielding occurs at a slower pace compared with developments in the missile force, given priority and systemic resource constraints. In 2023, North Korea showcased new UAV systems that appear similar to the U.S. MQ-9 Reaper and Global Hawk, though the technical capability probably is limited compared to the U.S. systems.

Kim will continue to prioritize efforts to build a more capable missile force—from cruise missiles through ICBMs, and hypersonic glide vehicles—designed to evade U.S. and regional missile defenses and imports a variety of dual-use goods in violation of UN sanctions, primarily from China and Russia.

- In 2023, North Korea launched its ballistic missile submarine following years of modifying an old Romeo-class submarine. Kim has stated his intention to convert more submarines for a similar mission.
- In January 2024, Pyongyang launched a new, solid-propellant missile that it claims is an intermediate-range ballistic missile equipped with a maneuverable, hypersonic reentry vehicle.
- In 2023, North Korea launched three SLVs, two failed and the third successfully placed a satellite in orbit.
- In 2023, North Korea conducted five flight tests of its ICBMs, including the Hwasong-15 and Hwasong-17 liquid-propellant ICBMs as well as its new solid-propellant ICBM, the Hwasong-18.

Cyber

North Korea's cyber program will pose a sophisticated and agile espionage, cybercrime, and attack threat. Pyongyang's cyber forces have matured and are fully capable of achieving a variety of strategic objectives against diverse targets, including a wider target set in the United States and South Korea.

North Korea will continue its ongoing cyber campaign, particularly cryptocurrency heists; seek a broad variety of approaches to launder and cash out stolen cryptocurrency; and maintain a program of IT workers serving abroad to earn additional funds.

Challenges

While North Korea has managed to weather the effects of the pandemic and its extreme self-imposed isolation; in the long term, Kim will have to balance his desire for absolute state control

[22]

with the negative impact upon his country's economic well-being. The Kim regime has prioritized recentralizing authority above its population and its economy with brutal crackdowns and serious mismanagement of agriculture that probably are worsening living conditions. The North Korean regime has long feared losing control over its people and is trying to roll back the relatively modest levels of private economic activity that have arisen since the 1990s and to ensure state domination over everyday life.

- The regime's recentralization campaign is meant to ensure the long-term survival of Kim-family rule. Its intensity stems from the collapse of fellow communist dictatorships during the 1990s in which the gradual erosion of authority and infiltration of foreign ideas eventually undermined the state. The crackdown restricts livelihoods and promotes inefficient state controls, contributing to food shortages and some decline in civil order—particularly violent crime.

CONFLICTS AND FRAGILITY

Preface

The potential for interstate conflict and domestic turmoil in other countries around the world also continues to pose challenges for U.S. national security, both directly and as threats to our allies and partners. Rising tension and instability from these flashpoints can be exacerbated by the intensifying global power competition given the complex and interconnected security landscape. Conflicts, particularly those that disrupt global trade and investment flows, might lead to rising energy prices and increased economic fragility even in countries that are not directly involved or are far removed from the conflict. For example, tourism, which is a major foreign exchange earner for Egypt, Jordan, and Lebanon, has fallen sharply since the onset of the Gaza conflict and disruptions in Ukrainian food exports in 2022 helped to fuel rising global food prices. Regional and localized conflicts have far-reaching and sometimes cascading implications for not only neighboring countries, but also the world. In addition to being illustrative of this phenomenon, the ongoing conflict in Gaza also highlights the potential for spillover into larger and more dangerous conflict.

Gaza Conflict

The HAMAS attack against Israel in October 2023 and Israel's responding military campaign in Gaza has increased tensions throughout the region as Iranian proxies and partners conduct anti-U.S. and anti-Israel attacks, both in support of HAMAS and to pressure the United States. Media coverage of the destruction and loss of life are being amplified by active social media campaigns on all sides, roiling public reactions among neighboring countries and around the world. Israel will face mounting international pressure because of the dire humanitarian situation in the Gaza Strip, and Iranian-backed attacks will jeopardize stability in Lebanon, Iraq, the Gulf, and the Red Sea. The risk of escalation into direct interstate conflict, intended or otherwise, remains high.

- The Gaza conflict is posing a challenge to many key Arab partners, who face public sentiment against Israel and the United States for the death and destruction in Gaza, but also see the United States as the power broker best positioned to deter further aggression and end the conflict before it spreads deeper into the region.

Israel and Iran are trying to calibrate their actions against each other to avoid escalation into a direct full-scale conflict. We assess that Iranian leaders did not orchestrate nor had foreknowledge of the HAMAS attack against Israel.

Since October 2023, Iran has encouraged and enabled its various proxies and partners—including Hizballah, Iranian-backed groups in Iraq and Syria, and the Huthis in Yemen—to conduct strikes against Israeli or U.S. interests in the region.

- Hizballah is calibrating this pressure on Israel from the north while trying to avoid a broader war that would devastate Hizballah and Lebanon. Hizballah's leadership, though, probably will consider a range of retaliatory options depending on Israel's actions in Lebanon during the upcoming year.

[24]

- In Iraq, Iranian-aligned militias almost certainly will continue attacks against U.S. forces in Iraq and Syria.
- The Huthi's continued ballistic missile, cruise missile, and UAV attacks against merchant vessels transiting the Red Sea, which are disrupting international shipping, and on Israel create a real risk of broader escalation.

Both al-Qa'ida and ISIS, inspired by the HAMAS attack against Israel, have directed their supporters to conduct attacks against Israeli and U.S. interests. The HAMAS attack is encouraging individuals to conduct acts of antisemitic and Islamophobic terror worldwide and is galvanizing individuals to leverage the Palestinian plight for recruitment and inspiration to conduct attacks. The Nordic Resistance Movement—a transnational neo-Nazi organization—publicly praised the attack, illustrating the conflict's appeal to a range of threat actors.

In regard to Gaza, Jerusalem remains focused on destroying HAMAS, which its population broadly supports. Moreover, Israel probably will face lingering armed resistance from HAMAS for years to come, and the military will struggle to neutralize HAMAS's underground infrastructure, which allows insurgents to hide, regain strength, and surprise Israeli forces.

The governance and security structures in Gaza and the West Bank as well as the resolution of the humanitarian situation in Gaza and rebuilding will be key components of the long-term Israeli–Palestinian relationship.

- Israeli Prime Minister Binyamin Netanyahu has publicly stated his opposition to postwar diplomacy with the Palestinian Authority (PA) toward territorial compromise.
- Netanyahu's viability as leader as well as his governing coalition of far-right and ultraorthodox parties that pursued hardline policies on Palestinian and security issues may be in jeopardy. Distrust of Netanyahu's ability to rule has deepened and broadened across the public from its already high levels before the war, and we expect large protests demanding his resignation and new elections. A different, more moderate government is a possibility.

HAMAS's and the PA's continued animosity will be a factor in governance outcomes as will HAMAS's broad popular support. Much also will hinge on Israel's decisions regarding how to deal with Gaza in the aftermath of its campaign as well as scale and scope of its support for the PA.

Potential Interstate Conflict

Interstate conflict can have broader cascading security, economic, and humanitarian implications on a regional and even global scale. The following are a few of the potential conflicts between states that could spill over with repercussions that may require immediate U.S. attention.

China Maritime

Beijing's efforts to try to assert sovereignty claims over islands in the South and East China Seas will result in persistently high tension between the PRC and its neighboring competing claimants and increase opportunities for miscalculation, even though Beijing probably prefers to avoid direct conflict. Beijing

maintains a maritime presence near contested areas, and its military bases in the Spratly Islands allow for a sustained presence in disputed areas and provide the capability to rapidly react to crises in the South China Sea.

- In 2023, the PRC Coast Guard used water cannons and floating barriers to block Filipino access to disputed areas in the South China Sea. The PRC's collisions with Filipino supply ships generated media attention that highlighted China's aggressive behaviors. Manila is unlikely to relinquish its outpost at Second Thomas Shoal presenting more opportunities for inadvertent escalation by either side.

- Tension between China and Japan over the Senkaku Islands last flared up a decade ago. Since then, Chinese ships have constantly remained in the proximity of the disputed islands, occasionally entering the territorial zone, and driving responses from Japan's Self-Defense Force to monitor the activity.

India–China

The shared disputed border between India and China will remain a strain on their bilateral relationship. While the two sides have not engaged in significant cross-border clashes since 2020, they are maintaining large troop deployments, and sporadic encounters between opposing forces risk miscalculation and escalation into armed conflict.

India–Pakistan

New Delhi and Islamabad are inclined to sustain the current fragile calm in their relationship following their renewal of a cease-fire along the Line of Control in early 2021. However, neither side has used this period of calm to rebuild their bilateral ties as each government has focused on more pressing domestic priorities including election perpetrations and campaigning and for Pakistan, concerns over rising militant attacks in its west. Pakistan's long history of supporting anti-India militant groups and India's increased willingness, under the leadership of Prime Minister Narendra Modi, to respond with military force to perceived or real Pakistani provocations raise the risk of escalation during a crisis. There remains the potential for an event to trigger a rapid escalation.

Azerbaijan–Armenia

Relations between Armenia and Azerbaijan are likely to remain tense, but Azerbaijan's retaking of Nagorno-Karabakh (N-K) has reduced volatility, and a military confrontation probably would be limited in duration and intensity. Nevertheless, the lack of a bilateral peace treaty, the proximity of their military forces, the lack of a cease-fire enforcement mechanism, and Azerbaijan's readiness to use calibrated military pressure to advance its goals in talks with Armenia will remain. Moreover, the transition of N-K governance from ethnic Armenians to Azerbaijanis and Azerbaijan's demand for access to a land corridor linking Azerbaijan to its exclave will elevate the risk of armed confrontation.

- In September 2023, Azerbaijan initiated a military operation that led to the defeat of the N-K Self Defense Force and the surrender of the de facto N-K authorities. The rapid exodus of most of the region's ethnic Armenian population and the planned self-dissolution of the

government allowed Baku to advance plans to integrate the region with Azerbaijan, effectively removing this longstanding issue from the bilateral peace agenda.

Potential Intrastate Turmoil

Intrastate turmoil—whether grounded in domestic unrest, economic discontent, or governance challenges—can fuel cycles of violence, insurgencies, and internal conflict. The challenges often are intertwined with diminished socioeconomic performance, endemic corruption, population dislocations, pressures from climate change, and the spread of extremists' ideologies from terrorist and insurgent groups. During the past decade, an erosion of democracy around the world, strains in U.S. alliances, and challenges to international norms have made it more difficult for the United States and its allies to tackle global issues while creating greater opportunities for rogue governments and groups to operate with impunity. Below we highlight a few instances that will have the potential for greater impact on global security and the potential for action from the United States, its allies, and partners.

The Balkans

The Western Balkans probably will face an increased risk of localized interethnic violence during 2024. Nationalist leaders are likely to exacerbate tension for their political advantage and outside actors will reinforce and exploit ethnic differences to increase or protect their regional influence or thwart greater Balkan integration into the EU or Euro–Atlantic institutions.

- Clashes between Serb nationalists and Kosovar authorities have led to deaths and injuries, including injuries to NATO peacekeepers, in 2023.
- Bosnian Serb leader Milorad Dodik is taking provocative steps to neutralize international oversight in Bosnia and secure de facto secession for his Republika Srpska. His action could prompt leaders of the Bosniak (Bosnian Muslim) population to bolster their own capacity to protect their interests and possibly lead to violent conflicts that could overwhelm peacekeeping forces.

Afghanistan

The Taliban regime has strengthened its power in Afghanistan, suppressed anti-Taliban groups, bolstered international engagement, and will continue to prioritize enforcement of theocratic rule. However, the Taliban will not adequately address Afghanistan's persistent humanitarian crisis or structural economic weaknesses.

- The Taliban will continue to implement restrictive measures, carry out public punishments, crack down on protests, and prevent most women and girls from attending secondary school and university. However, near-term prospects for regime-threatening resistance remain low because large swathes of the Afghan public are weary of war and fearful of Taliban reprisals, and armed remnants lack strong leadership and external support.

- Regional powers will continue to focus largely on keeping problems contained in Afghanistan and seek to develop transactional arrangements with the Taliban while proceeding cautiously with Taliban requests for formal recognition.

Sudan

Prolonged conflict heightens the risks of conflict spreading beyond Sudan's borders, external actors joining the fray, and civilians facing death and displacement. The Sudanese Armed Forces and Rapid Support Forces are still fighting because their leaders calculate that they can achieve their goals absent a negotiated cessation of hostilities. With Sudan at the crossroads of the Horn of Africa, the Sahel, and North Africa, it could once again become an ideal environment for terrorist and criminal networks.

- Sudan's warring security forces may be receiving more foreign military support, which is likely to hamper progress on any future peace talks. Any increased involvement by one external actor could prompt others to quickly follow suit.

Ethiopia

Ethiopia is undergoing multiple, simultaneous internal conflicts, heightening interethnic tension and the risk of atrocities against civilians. A new conflict emerged in the Amhara Regional State in April 2023, when the Ethiopian Government clashed with Amhara militia and fighting persisted throughout the year. While the Cessation of Hostilities Agreement in November 2022 between the Ethiopian Government and the Tigrayans ended a two-year war, unresolved territorial issues could lead to a resumption of conflict.

The Sahel

Since 2020, the Sahel has experienced seven irregular transfers of power because leaders have failed to address poor governance and public grievances or adequately resourced their militaries to achieve their missions. This turmoil raises the likelihood that these crises will metastasize and spillover to neighboring countries in Coastal West Africa in 2024. Many Coastal West African governments are facing potential coups because of lingering civil-military strains, growing public dissatisfaction with their failure to deliver improved governance and living standards, and an increase in foreign partners willing to condone military rule to focus on narrow security interests. Future coup leaders most likely will calculate that competition among major powers will create the space to weather any international fallout.

- Russia has opportunistically capitalized on domestic turmoil, offering rhetorical and, in some instances, substantive support to those seeking to oust regimes.

- Mounting crises are beginning to fray regional institutions, further hampering their ability to develop effective regional security responses. In 2023, juntas in Burkina Faso, Mali, and Niger formed a separate alliance to buck pressure from the Economic Community of West African

States (ECOWAS), historically one of the most consistent bodies in trying to uphold anti-coup norms in the region.

- Several Western partners are focusing on core security interests in the region—such as stemming migrant flows, containing geopolitical rivals, and CT gains—at the expense of longer-term support to democracy and governance.

Haiti

Conditions will remain unpredictable as weak government institutions lose their grip on power to gang territorial control, particularly in the capital Port-au-Prince. This will be coupled with an eroding economy, infrastructure, and an increasingly dire humanitarian situation. Gangs will be more likely to violently resist a foreign national force deployment to Haiti because they perceive it to be a shared threat to their control and operations.

- Top Haitian gang leaders such as G-9 leader Jimmy "Barbeque" Cherizier and Kraze Barye leader Vitelhomme Innocent have called for the overthrow of Prime Minister Ariel Henry's government.

- The Haitian National Police has been unable to counter gang violence and has been plagued by resource issues, corruption challenges, and limited training.

Venezuela

Disputed Venezuelan President Nicolas Maduro will retain a solid hold on power and is unlikely to lose the 2024 presidential election because of his control of state institutions that influence the electoral process and his willingness to exercise his power. The opposition, which has often been divided, holds few public positions of influence.

- Support from China, Iran, and Russia help the Maduro regime evade sanctions.

- So far, the regime has banned top opposition candidates from holding public office, restricted media coverage of opposition politicians, and placed close allies in the National Electoral Council to ensure Maduro's victory while also trying to avoid blatant voting fraud.

More than 7.7 million Venezuelans have left the country since 2017, 6.5 million of whom are living in Latin America and the Caribbean. Venezuelan emigration to the region and the United States is likely to remain elevated through next year as the lack of economic opportunities are likely to persist.

- More than 80 percent of Venezuelans have incomes below the poverty line and low-levels of economic growth would be insufficient to lift most out of poverty or mitigate drivers of migration.

TRANSNATIONAL ISSUES

PREFACE

Transnational threats interact in a complex system along with threats from state-actors, often reinforcing each other and creating compounding and cascading risks to U.S. national security. Increasing interconnections among countries also have created new opportunities for transnational interference and conflict. Several clear and direct challenges are the rapid development of technologies, the spread of repression beyond physical borders, the threats posed by transnational organized crime and terrorism, and the societal effects of international migration.

CONTESTED SPACES

Disruptive Technology

New technologies—particularly in the fields of AI and biotechnology—are being developed and are proliferating at a rate that makes it challenging for companies and governments to shape norms regarding civil liberties, privacy, and ethics. The convergence of these emerging technologies is likely to create breakthroughs, which could lead to the rapid development of asymmetric threats—such as advanced UAVs—to U.S. interests and probably will help shape U.S. economic prosperity.

- For example, stealth technology has significantly impacted conventional defense systems and has driven the efforts of varying countries to start a new round of research on detection systems and guided weapons. A key trend is the development of advanced materials with enhanced stealth properties with reduced reflection and absorption properties.

Advances in AI and new machine learning models are moving AI into its industrial age, with potentially huge economic impacts for both winners and followers and unintended consequences—from rampant deepfakes and misinformation to the development of AI-generated computer viruses or new chemical weapons. Generative AI is a means for discovering and designing novel technologies and advanced system-level processes that could strengthen a country's technological, economic, and broader strategic competitiveness.

- China is pursuing AI for smart cities, mass surveillance, healthcare, drug discovery, and intelligent weapons platforms. Chinese AI firms are already world leaders in voice and image recognition, video analytics, and mass surveillance technologies.

- PRC researchers have described the application of generative AI to drug discovery as "revolutionary." On average, it takes more than 10 years and billions of dollars to develop a new drug. AI can make drug discovery faster and cheaper by using machine-learning models to predict how potential drugs might behave in the body and cut down on the need for painstaking lab work on dead-end compounds.

[30]

- Russia is using AI to create deepfakes and is developing the capability to fool experts. Individuals in warzones and unstable political environments may serve as some of the highest-value targets for such deepfake malign influence.

Innovators in synthetic biology probably will control new military and commercial applications and hold trillions of dollars in production capacity, including supply chains for products that vary from disease-resistant crop seeds to metals to pharmaceuticals.

- Countries, such as China and the United States, that lead biotechnological breakthroughs in fields such as precision medicine, synthetic biology, big data, and biomimetic materials, will not only drive industry growth, but also international competition and will exert substantial influence over the global economy for generations.

Digital Authoritarianism and Transnational Repression

Foreign states are advancing digital and physical means to repress individual critics and diaspora communities abroad, including in the United States, to limit their influence over domestic publics. States are also growing more sophisticated in digital influence operations that try to affect foreign publics' views, sway voters' perspectives, shift policies, and create social and political upheaval. Digital technologies have become a core component of many governments' repressive toolkits even as they continue to engage in physical acts of transnational repression, including assassinations, abductions, abuse of arrest warrants and familial intimidation. The PRC probably is the top perpetrator of physical transnational repression.

- During the next several years, governments are likely to exploit new and more intrusive technologies—including generative AI—for transnational repression. From 2011 to 2023, at least 74 countries contracted with private companies to obtain commercial spyware, which governments are increasingly using to target dissidents and journalists.

- PRC expatriates have faced accusations of false bomb threats in countries around the world, resulting in local police investigations, revoked visas, placement on travel blacklists, and sometimes detention, as means to harass dissidents overseas. The PRC also probably will seek to maintain its public security bureaus also known as "overseas police stations" to monitor and repress the Chinese diaspora.

WMD

Nuclear Weapons

The expansion of nuclear weapons stockpiles and their delivery systems, coupled with increasing regional conflicts involving nuclear weapons states, pose a significant challenge to global efforts to prevent the spread and use of nuclear weapons. Arms control efforts through 2035 will change in scope and complexity as the number of strategic technologies and the countries that have them grow.

[31]

- China and Russia are seeking to ensure strategic stability with the United States through the growth and development of a range of weapons capabilities, including nontraditional weapons intended to defeat or evade U.S. missile defenses.

- North Korea continues to threaten to conduct a seventh nuclear test and the potential for heightened tension between Pakistan and India could increase the risk of nuclear escalation.

Chemical Weapons

The use of chemical weapons, particularly in situations other than state-on-state military operations, could increase in the near future. During the past decade, state and non-state actors have used chemical warfare agents in a range of scenarios, including the Syrian military's use of chlorine and sarin against opposition groups and civilians, and North Korea's and Russia's use of chemical agents in targeted killings. More state actors could use chemicals in operations against dissidents, defectors, and other perceived enemies of the state; protestors under the guise of quelling domestic unrest; or against their own civilian or refugee populations.

Biological Weapons

Current biological agents and rapidly advancing biotechnology underscore the diverse and dynamic nature of deliberate biological threats. Rapid advances in dual-use technology, including bioinformatics, synthetic biology, nanotechnology, and genomic editing, could enable development of novel biological threats.

- Russia, China, Iran, and North Korea probably maintain the capability to produce and use pathogens and toxins, and China and Russia have proven adept at manipulating the information space to reduce trust and confidence in countermeasures and U.S. biotechnology and research.

[32]

SHARED DOMAINS

Environmental Change and Extreme Weather

The risks to U.S. national security interests are increasing as the physical effects of climate and environmental change intersect with geopolitical tension and vulnerabilities of some global systems. Climate-related disasters in low-income countries will deepen economic challenges, raise the risk of inter-communal conflict over scarce resources, and increase the need for humanitarian and financial assistance.

- Climate-related disasters and economic losses in low-income countries are poised to continue contributing to cross-border migration.
- Competition over access and economic resources in the Arctic, as sea ice recedes, increases the risk of miscalculation, particularly while there is military tension between Russia and the other seven countries with Arctic territory.
- El Nino weather patterns are combining with the effects of climate change and pre-existing vulnerabilities in critical infrastructure to worsen populations' exposure to flooding, drought, heatwaves, and intense storms. El Nino-related events are projected to reduce global economic growth, resulting in more than $3 trillion in lost GDP during the rest of the decade.
- Droughts are decreasing shipping capacity and energy generation in Central America, China, Europe, and the United States, and insurance losses from catastrophes have increased 250 percent during the past 30 years.
- Changing weather patterns' effects on major agricultural exporters and important local agricultural areas may put more stress on food systems in vulnerable areas of Africa, Latin America, and South Asia. The sustainable fish stocks on which some coastal populations depend are declining because of rising ocean temperatures and overfishing, particularly by illegal, unreported, and unregulated (IUU) fishing.

Intensifying effects of climate change—combined with El Nino weather patterns—are likely to exacerbate risks to human health, primarily but not exclusively, in low- and middle-income countries. Rising land and ocean temperatures, changing precipitation patterns, and increased frequency of severe weather events are likely to intersect with environmental degradation, pollution, and poor resource management to exacerbate food and water insecurity, malnutrition, and disease outbreaks.

Health Security

National health system shortfalls, public mistrust and medical misinformation, and eroding global health governance will impede the capacity of countries to respond to health threats. Countries remain vulnerable to the introduction of a new or reemerging pathogen that could cause another devastating pandemic.

- The predicted shortage of at least 10 million healthcare workers by 2030 will occur primarily in low- and middle-income countries.
- Global health governance and adherence to UN health protocols may be eroded during the coming year by continued disregard by governments of international health institutions and norms and adversary interference in global health initiatives.
- Drivers for infectious disease emergence are on the rise, including deforestation, wildlife harvesting and trade, mass food production, and lack of international consensus on biosafety norms. These drivers are compounded by factors that facilitate global spread, such as international travel and trade, inadequate global disease surveillance and control, weakened health systems, public distrust, and medical misinformation.
- Significant outbreaks of highly pathogenic avian influenza, cholera, dengue, Ebola, monkeypox, and polio have stretched global and national disease detection and response systems further straining the international community's ability to address health emergencies.

Our Assessment of the Origins of COVID-19

The IC continues to investigate how SARS-CoV-2, the virus that causes COVID-19, first infected humans. All agencies assess two hypotheses are plausible: natural exposure to an infected animal and a laboratory-associated incident.

- The National Intelligence Council and four other IC agencies assess that the initial human infection with SARS-CoV-2 most likely was caused by natural exposure to an infected animal that carried SARS-CoV-2 or a close progenitor, a virus that probably would be more than 99 percent similar to SARSCoV-2. The Department of Energy and the FBI assess that a laboratory-associated incident was the most likely cause of the first human infection with SARS-CoV-2, although for different reasons. The CIA and another agency remain unable to determine the precise origin of the COVID-19 pandemic, as both hypotheses rely on significant assumptions or face challenges with conflicting reporting.
- Beijing continues to resist sharing critical and technical information about coronaviruses and to blame other countries, including the United States, for the pandemic.

Anomalous Health Incidents

We continue to closely examine anomalous health incidents (AHIs), particularly in areas we have identified as requiring additional research and analysis. Most IC agencies have concluded that it is very unlikely a foreign adversary is responsible for the reported AHIs. IC agencies have varying confidence levels because we still have gaps given the challenges collecting on foreign adversaries—as we do on many issues involving them. As part of its review, the IC identified

[34]

critical assumptions surrounding the initial AHIs reported in Cuba from 2016 to 2018, which framed the IC's understanding of this phenomenon, but were not borne out by subsequent medical and technical analysis. In light of this and the evidence that points away from a foreign adversary, causal mechanism, or unique syndromes linked to AHIs, IC agencies assess those symptoms reported by U.S. personnel probably were the result of factors that did not involve a foreign adversary.

- These findings do not call into question the very real experiences and symptoms that our colleagues and their family members have reported. We continue to prioritize our work on such incidents, allocating resources and expertise across the government, pursuing multiple lines of inquiry and seeking information to fill the gaps we have identified.

Migration

Conflict, violence, political instability, poor economic conditions, and natural disasters will continue to displace growing numbers of people within their own national borders and internationally—straining countries' capacity to absorb new arrivals and governments' abilities to provide services and manage domestic public discontent. The Western Hemisphere most likely will continue to sustain high levels of intra-regional migrant flows driven by poor socioeconomic conditions and insecurity as well as pull factors that include economic opportunity, family reunification, and perceptions of immigration policies in recipient or transit countries.

- The number of individuals internally displaced from their homes in 2022 was more than three times higher than the average of the previous 10 years. Irregular migration to high-income countries is increasing as several countries in Africa, Latin America, and the Caribbean experience political turmoil and poor economic performance.

- Political repression and lack of economic opportunities will continue to drive Cuban, Nicaraguan, and Venezuelan emigration; however, those regimes will continue to blame U.S. sanctions and policies for irregular emigration from their countries.

- Changes to Western Hemisphere countries' visa requirements—such as Nicaragua's relaxation of requirements for nationals from Haiti—could trigger new surges in U.S.-bound irregular migration.

NON-STATE ACTOR ISSUES

Transnational Organized Crime

Transnational criminal organizations (TCOs) threaten U.S. and allied public health systems, exploit the international financial system, and degrade the safety and security of the United States and partner nations. TCOs incite instability and violence, drive migration, and provide some U.S. adversaries with additional avenues to advance their geopolitical interests.

Foreign Illicit Drugs

Western Hemisphere-based TCOs involved in illicit drug production and trafficking bound for the United States and partner nations, endanger the health and safety of millions of individuals and contribute to a global health crisis. Illicit drugs including fentanyl, heroin, methamphetamine, and South American-sourced cocaine all contribute to global demand for drugs.

- Mexico-based TCOs are the dominant producers and suppliers of illicit drugs to the U.S. market, including fentanyl, heroin, methamphetamine, and South American-sourced cocaine.
- Both Colombia and Ecuador are impacted by record levels of cocaine being produced and trafficked to international markets contributing to a global drug demand, while fueling drug related violence within their borders.

Fentanyl

Illicit fentanyl will continue to pose a major threat to the health of Americans. In 2023, a majority of the more than 100,000 annual drug overdose deaths in the United States are attributed to illicit fentanyl mostly supplied by Mexican-based TCOs, even as U.S. law enforcement seized record amounts of illicit fentanyl, precursor chemicals, and pill pressing equipment.

- Mexico-based TCOs are the dominant producers of illicit fentanyl for the U.S. market, although there also are independent illicit fentanyl producers, and the fragmentation of fentanyl operations has made disruption efforts challenging. Some aspects of fentanyl production are spilling over into the United States with drug traffickers conducting the finishing stages of fentanyl pill packing or pressing in the United States.
- China remains the primary source for illicit fentanyl precursor chemicals and pill pressing equipment. Brokers circumvent international controls through mislabeled shipments and the purchase of unregulated dual-use chemicals. However, Mexico-based TCOs also are sourcing precursor chemicals to a lesser extent from other nations such as India.

Money Laundering and Financial Crimes

TCOs are defrauding individuals, businesses, and government programs, while laundering billions of dollars of illicit proceeds through U.S. financial institutions. Their fraud schemes and tactics vary

[36]

widely. Some use shell and front companies to obfuscate their illicit activities and some TCOs rely on professional money launderers or financial experts and other tactics to launder illicit proceeds.

- TCOs still rely on traditional money laundering methods and bulk cash smuggling operations to repatriate drug proceeds from the United States, while some money launderers are using cryptocurrency transactions.

Cyber Crime

Transnational organized criminals involved in ransomware operations are improving their attacks, extorting funds, disrupting critical services, and exposing sensitive data. Important U.S. services and critical infrastructure such as health care, schools, and manufacturing continue to experience ransomware attacks; however, weak cyber defenses, coupled with efforts to digitize economies, have made low-income countries' networks also attractive targets.

- The emergence of inexpensive and anonymizing online infrastructure combined with the growing profitability of ransomware has led to the proliferation, decentralization, and specialization of cyber criminal activity. This interconnected system has improved the efficiency and sophistication of ransomware attacks while also lowering the technical bar for entry for new actors.

- Transnational organized criminals sometimes cease operations temporarily in response to high-profile attention, law enforcement action, or disruption of infrastructure, although group members also find ways to rebrand, reconstitute, or renew their activities.

- Absent cooperative law enforcement from Russia or other countries that provide cyber criminals a safe haven or permissive environment, mitigation efforts will remain limited.

Undermining Rule of Law

TCOs and criminal gangs undermine the rule of law through exploiting corruption networks, committing acts of violence, and overpowering regional security forces. TCOs regularly co-opt foreign government officials through bribes or threats to create a permissive operating environment and target officials who support stronger counter-drug efforts.

- TCOs bribe foreign political candidates and security officials in an effort to limit enforcement actions and to protect illicit operations, such as illicit drug production or cross-border smuggling operations.

- Drug-related gang violence in Ecuador has led to surging homicide rates and the assassination of a presidential candidate. The nation has declared multiple states of emergency, suspending essential public services—including public transportation—and closing schools and businesses.

Human Trafficking

TCOs and criminal actors view human trafficking, including sex trafficking and forced labor, as low risk crimes of opportunity. Multiple criminal actors engage in operations that seek to exploit vulnerable

individuals and groups to bolster illicit revenue streams. TCOs that engage in human trafficking may also engage in drug trafficking, weapons smuggling, human smuggling, and money laundering.

- Human traffickers typically coerce or defraud their victims into sex trafficking or forced labor, confiscating identification documents and requiring the payment of debts. In 2023, U.S. law enforcement officials noted multiple incidents where unaccompanied minors were exploited in forced labor operations in U.S. food processing plants to pay off debts.

- TCOs based in the Western Hemisphere and Asia are most likely to engage in human trafficking activity with ties to the United States.

Migrants transiting the Western Hemisphere to the United States are exploited by criminal actors through kidnapping for ransom, targets of forced labor, or victims of sex trafficking operations. TCOs, human smugglers, gangs, and lone criminal actors are all taking advantage of elevated levels of U.S.-bound migration, and vulnerable migrants are at risk of being trafficked.

- Some migrants, who voluntarily use human smuggling networks to facilitate their travel to the United States, are trafficked during their journey.

Global Terrorism

U.S. persons and interests at home and abroad will face an ideologically diverse threat from terrorism. This threat is mostly likely to manifest in small cells or individuals inspired by foreign terrorist organizations and violent extremist ideologies to conduct attacks. While al-Qa'ida has reached an operational nadir in Afghanistan and Pakistan and ISIS has suffered cascading leadership losses in Iraq and Syria, regional affiliates will continue to expand. These gains symbolize the shift of the center of gravity in the Sunni global jihad to Africa.

- Terrorists will maintain an interest in conducting attacks using chemical, biological and radioactive materials against U.S. persons, allies, and interests worldwide. Terrorists from diverse ideological backgrounds continue to circulate instructions of varied credibility for the procurement or production of toxic or radioactive weapons using widely available materials in social media and online fora.

ISIS

ISIS will remain a centralized global organization even as it has been forced to rely on regional branches in response to successive leadership losses during the past few years. External capabilities vary across ISIS's global branches, but the group will remain focused on attempting to conduct and inspire global attacks against the West and Western interests.

- ISIS–Greater Sahara and ISIS–West Africa contribute to and capitalize on government instability, communal conflict, and anti-government grievances to make gains in Nigeria and the Sahel.

- ISIS-Khorasan is trying to conduct attacks that undermine the legitimacy of the Taliban regime by expanding attacks against foreign interests in Afghanistan.

[38]

Al-Qa'ida

Al-Qa'ida's regional affiliates on the African continent and Yemen will sustain the global network as the group maintains its strategic intent to target the United States and U.S. citizens. Al-Qa'ida senior leadership has not yet announced the replacement for the former emir, Ayman al-Zawahiri, reflecting the regionally focused and decentralized nature of the organization.

- Al-Shabaab continues to advance its attack capabilities by acquiring weapons systems while countering a multinational CT campaign, presenting a risk to U.S. personnel. In 2023, al-Shabaab also expanded its operations in Northeast Kenya.

Hizballah

Lebanese Hizballah will continue to develop its global terrorist capabilities as a complement to the group's growing conventional military capabilities in the region. Since October 2023, Hizballah has conducted attacks along Israel's northern border to tie down Israeli forces as they seek to eliminate HAMAS in Gaza. Hizballah probably will continue to conduct provocative actions such as rocket launches against Israel throughout the conflict.

- Hizballah seeks to limit U.S. influence in Lebanon and the broader Middle East, and maintains the capability to target U.S. persons and interests in the region, worldwide, and, to a lesser extent, in the United States.

Transnational Racially or Ethnically Motivated Violent Extremists

The transnational racially or ethnically motivated violent extremists (RMVE) movement, in particular motivated by white supremacy, will continue to foment violence across Europe, South America, Australia, Canada, and New Zealand inspiring the lone actor or small-cell attacks that pose a significant threat to U.S. persons. The loose structure of transnational RMVE organizations and networks, which encourage or inspire but do not typically direct attacks, will challenge local security services and creates resilience against disruptions.

- Lone actors are difficult to detect and disrupt because of their lack of affiliation. While these violent extremists tend to leverage simple attack methods, they can have devastating, outsized consequences.

- RMVE publications and manifestoes from previous attackers feed the RMVE movement with violent propaganda, targets, and tactics. The Terrorgram Collective, a loosely connected network of online channels and chatrooms, has a global reach and with its sophisticated online publications seek to inspire violence.

- Since early 2022, we have identified five RMVE attacks and five suspected RMVE attacks, killing a total of 27 people, by apparent lone actors in the United States and abroad. During the same period, there have been disrupted RMVE plots, arrests, and threats reported in several European countries.

Private Military and Security Companies

PMSCs are a growing presence in the international environment, and a handful of these firms associated with U.S. rivals, such as Russia, threaten global security in many countries and regions through their ability to potentially foment violence and escalate instability in already fragile regions

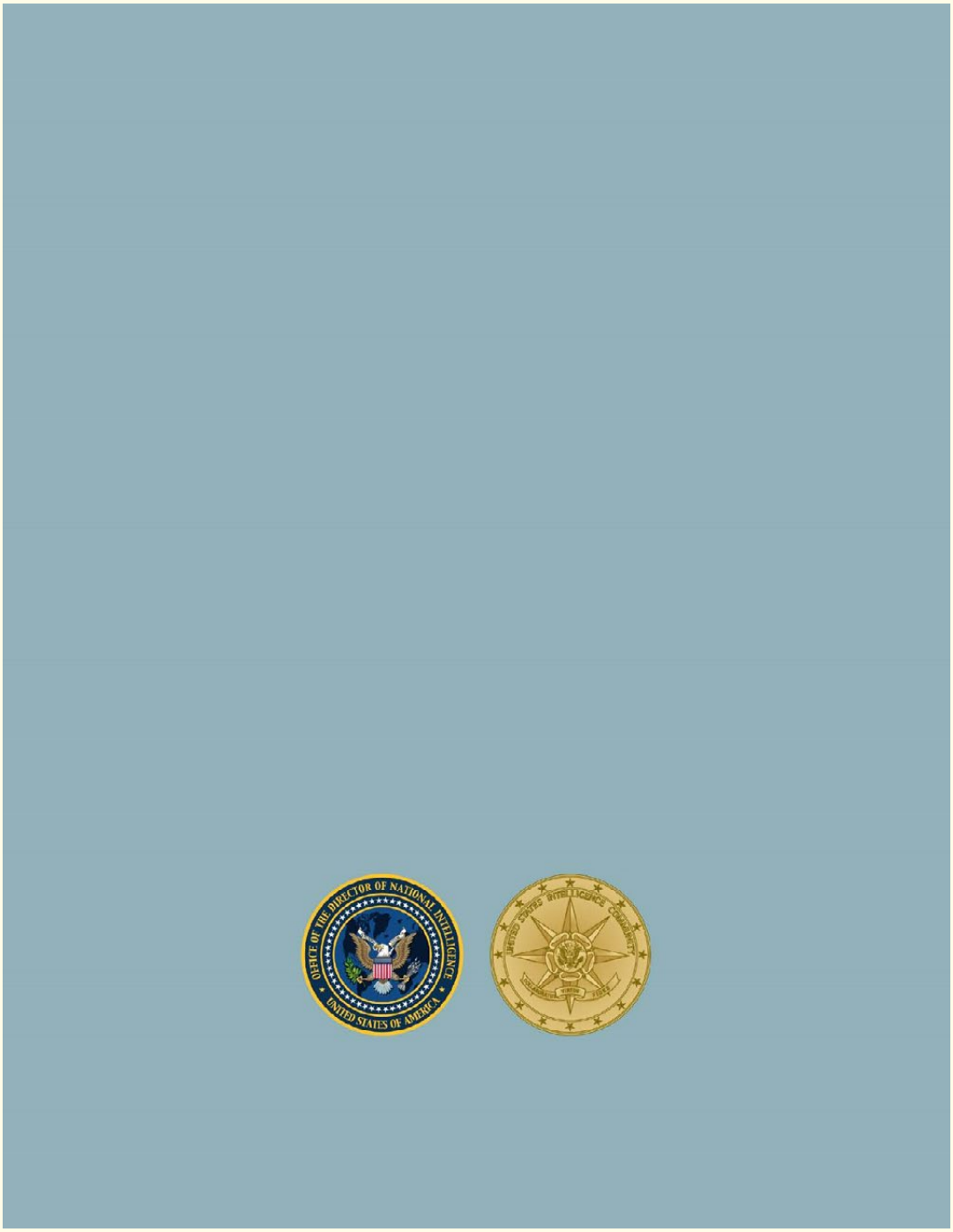
- PMSCs have become an essential component of modern military operations and the demand for their services is likely to grow. The largest part of the industry are corporations who provide for-hire security services for commercial interests or states. However, China, Russia, Turkey, and the UAE see PMSCs as a valuable tool in their arsenal for either advancing or protecting their interests abroad.

- Many governments will look to PMSCs to play an important role as a force multiplier for their conventional militaries—filling highly technical or manpower-intensive tasks such as maintenance, logistics, or fixed site security—or in some cases providing highly specialized, turn-key direct-action capabilities absent in their forces.

- Only a small number of PMSC contracts involve direct intervention, which are high-risk activities that may require the application of deadly force.

- No other PMSC has the funding sources, training, and size to operate on Vagner's scale as a proxy force, although a state actor could similarly scale a smaller PMSC's activities within one to two years.

[40]



Revista “Política y Estrategia” Nº 143, 2024, pp. 219-224
ISSN 0716-7415 (versión impresa) - ISSN 0719-8027 (versión en línea)
Academia Nacional de Estudios Políticos y Estratégicos
Conferencia de Seguridad de Múnich: el Alto Representante
Josep Borrell sobre la nueva agenda geopolítica
El Editor

CONFERENCIA DE SEGURIDAD DE MÚNICH: EL ALTO REPRESENTANTE JOSEP BORRELL SOBRE LA NUEVA AGENDA GEOPOLÍTICA

18.02.2024 Equipo de prensa del SEAE

La nueva, nueva agenda geopolítica. Si hace 50 meses, cuando asumí el cargo, alguien me hubiera preguntado: ‘¿Qué hay [en] tu nueva agenda geopolítica?’ seguro no hubiera dicho: voy a tener una pandemia. Voy a tener una guerra en Ucrania. Voy a tener una guerra en Gaza’. Nada de eso estaba previsto. Entonces, ¿cuál será la nueva [agenda geopolítica]? No sé.

Pero hablemos de lo que ya tenemos que afrontar. La agenda está determinada por los acontecimientos. Y los acontecimientos más importantes de hoy están relacionados con tres cuestiones geográficas, que son: Ucrania, Gaza y el Sur Global. Y una cuestión funcional, una cuestión estructural, que es la defensa.

De los tres desafíos geográficos, el primero [es] Ucrania. Tenemos que afrontar tres retos:

En primer lugar, tenemos que seguir apoyando a Ucrania militar y económicamente, más y más rápido. Tenemos que ser conscientes de que hay una guerra larga y de alta intensidad, en la que las bajas están aumentando en ambos bandos y en la que la tecnología está dando forma, a una velocidad increíble, al resultado de la guerra.

Estuve en Ucrania, en Kiev, hace unos días. Podría visitar las fábricas de drones y, seguro, el futuro de esta guerra estaría determinado por los drones y, en particular, por la introducción masiva de la inteligencia artificial en el campo de batalla.

Va a ser un nuevo tipo de guerra, donde [*no se oye*] ver las trincheras de la Primera Guerra Mundial, junto con la inteligencia artificial de Star Wars. Y llamaré la atención de nuestros ministros europeos sobre esa cuestión crucial. Hablamos de municiones y está claro que la munición de las armas clásicas es un tema muy importante. El presidente Zelensky habló de ello y tenemos que hacer más y más rápido al respecto -y no es porque nos falte capacidad, lo que nos falta es financiación- sino que tenemos que mirar hacia adelante, a los nuevos parámetros de la guerra.

En segundo lugar, tenemos que aumentar y proporcionar a Ucrania compromisos de seguridad. Los Estados miembros lo están haciendo, nosotros también estamos intentando hacerlo. Pero el compromiso de seguridad más importante para Ucrania es su membresía [en la UE]. Éste es un compromiso que asumimos con respecto a Ucrania. Será una Europa diferente con Ucrania dentro. Esto ha puesto en marcha todo el proceso de adhesión y tenemos que seguir comprometidos con ese compromiso.

El tercero es prepararnos para un largo período de tensiones con Rusia. Rusia puede verse tentada a incrementar sus provocaciones políticas y militares contra los países de la OTAN. Entonces, el mensaje es claro: tenemos un problema ruso por delante y para nosotros es un enorme desafío. Y para ello, nuestro esfuerzo militar debe mantenerse, en coo-

peración con un socio clave, como Estados Unidos. Pero tenemos que considerar diferentes escenarios sobre hasta qué punto Estados Unidos estará comprometido con la seguridad europea.

En Oriente Medio, debemos promover una solución política, integral, que incluya no sólo a Gaza sino también a Cisjordania.

Hemos estado hablando mucho, pero no tanto, de la situación en Oriente Medio. Y estoy sorprendido, porque todo el mundo habla de poner fin a la guerra en Gaza. Sí, tenemos que poner fin a la guerra en Gaza, pero nadie ha hablado mucho de Cisjordania. Y Cisjordania es el verdadero obstáculo para la solución de dos Estados.

Cisjordania está en ebullición. El nivel de violencia contra los palestinos ha ido aumentando desde el 7 de octubre. Antes de eso ya era muy alto. Y si ahora la UNRWA tiene que dejar de apoyar al pueblo palestino en Cisjordania, podríamos estar en vísperas de una explosión mayor.

La pregunta es: ¿Existe un espacio político para que Europa apoye una solución de dos Estados? Creo que lo hay. Pero para eso necesitamos estar más unidos. Si queremos desempeñar un papel geopolítico en esta cuestión, tenemos que estar más unidos, como lo hemos estado en el caso de Ucrania, donde -quizás con la excepción de un solo país- nuestra unidad ha sido notable. Pero aquí veo que hay una dispersión de enfoques y muchos Estados miembros quieren jugar su propio juego.

Tenemos que contar con Estados Unidos más que a bordo, pero tenemos que apoyar la iniciativa árabe. Hemos estado discutiendo mucho con los árabes y esperamos la propuesta del otro lado que los europeos podamos apoyar para que esta solución de dos Estados sea algo implementable. Llevamos 30 años hablando de ello, pero no hemos hecho –no diría nada, casi- nada para hacerlo realidad. Y sin ella no habrá paz en Oriente Medio. Sin unas perspectivas claras para el pueblo palestino, no habrá paz en Oriente Medio y la seguridad de Israel no podrá garantizarse sólo por medios militares.

Y el Sur Global, el tercero. Tienen su propia dinámica, pero no hay duda de que la guerra en Ucrania y Gaza ha aumentado enormemente el espacio político del Sur Global frente a nosotros. Y que tenemos que evitar ‹El resto contra Occidente›.

Para Rusia, este nuevo escenario geopolítico ha aumentado dramáticamente su posición desde el comienzo de la guerra en Gaza. Y realmente se están aprovechando de nuestros errores.

Culpan a los dobles raseros: esto es algo que debemos abordar y no sólo con palabras bonitas.

Está claro que el viento sopla en contra de Occidente, sopla en contra nuestra. Y tenemos que ganar la batalla de las narrativas, sobre Oriente Medio y Ucrania. Esas guerras son diferentes, con diferentes motivos, y diferentes causas porque son guerras por el territorio. Nos dijeron que la geografía ya no importa. Sí, importa. Estas guerras son guerras clásicas de personas que luchan por su tierra.

Surgirán muchos temas, pero más allá de estos tres desafíos discutiremos, una sola palabra sobre seguridad y defensa. Hace dos años lanzamos la Brújula Estratégica y dije: Europa está en peligro. Nadie le prestó mucha atención. Ahora todo el mundo habla de ello. Todo el mundo habla de seguridad y defensa, de un comisionado de defensa, de estructuras de defensa, de adquisiciones de defensa, de industria de defensa... Y con razón. No es muy pronto. Hemos estado en un largo período de desarme silencioso en Europa, silencioso. Poco a poco hemos ido perdiendo capacidad militar. Nuestra industria ha ido disminuyendo su capacidad.

Ahora está aumentando. En un año, un 40% más. No es suficiente, pero al menos vamos a un mejor ritmo. No podremos desempeñar un papel geopolítico si no somos capaces de defendernos. Y esto empieza por la industria y la ‹industria de la defensa› es algo importante, pero es diferente de la defensa. La defensa es competencia exclusiva de los Estados miembros.

Son los Estados miembros los que tienen un ejército. Son los Estados miembros los que tienen la capacidad de defensa. Y tenemos que hacer que trabajen mejor juntos, para tener más interoperabilidad y más coordinación, y la capacidad de lanzar misiones todos juntos. No para tener «un ejército europeo», sino para poder movilizar nuestros ejércitos (en plural) para afrontar los desafíos, cuando juntos podamos hacerlo mejor.

Durante mi mandato, lancé siete -siete- misiones civiles y militares de la Política Común de Seguridad y Defensa. Mi predecesor lanzó sólo uno. El próximo lunes lanzaremos otro al Mar Rojo, con el fin de dar seguridad a la navegación en estas zonas. Entonces, si queremos ser un actor geopolítico, debemos tener los medios. Y los medios empiezan por tener una fuerte capacidad de defensa. Al menos empiezan por tener una fuerte capacidad industrial de defensa.

Muchas gracias.

Preguntas y respuestas

¿Cree que la UE tendrá las capacidades, los hallazgos y la voluntad política para poder ser creíble?

Lo importante no es lo que creo. No es una cuestión de creencias. Es cuestión de tener voluntad. Y mi trabajo es, ha sido y seguirá siendo -durante al menos diez meses más- hacer entender a los Estados miembros que tienen que actuar juntos, más rápido y mejor. Las tres palabras clave: Juntos, más rápido y mejor.

Si no actúan juntos, serán más débiles. Pero trabajar juntos lleva demasiado tiempo. Para que funcionen juntos hay procedimientos que seguir, unanimidad que alcanzar… y todo eso lleva tiempo. Así que, al mismo tiempo, tenemos que poder aportar financiación, poner voluntad, cambiar los procedimientos y comprender que estamos -y no creo que lo entendamos- en una situación de guerra.

No creo que la gente del más alto nivel político, del nivel intermedio y de la opinión pública entiendan que estamos en una situación que requiere un modo y un enfoque completamente diferente, que no es simplemente: «Sí, lo haremos, pero «Ya veremos el próxi-

mo Consejo de Asuntos Exteriores, el mes que viene». No, dentro de tres meses las cosas se decidirán en el campo de batalla.

No podemos esperar a ‹veamos qué pasa en las elecciones europeas›; a ver, todavía no llegamos; queremos saber más detalles…›. Esto es para otra dimensión de la política. En la situación actual, la gente tiene que ser mucho más ágil, mucho más comprometida, mucho más directa. Tenemos muchas estrategias, pero no tenemos mucha acción.

En su presentación usted dijo: Si no puedes defenderte, no eres creíble. Se habla mucho, por ejemplo, de un Comisario de Defensa. ¿Cree que un Comisario de Defensa sería algo bueno?

Como dije antes, la defensa es competencia exclusiva de los Estados miembros. ¿Entendería usted tener un Comisario de Política Exterior de la Unión Europea? ¿No porque? Porque la Política Exterior es competencia de los Estados miembros. Pero lo que creo que es bueno tener es más acción por parte de la industria de defensa y hay competencia de la Comisión, porque la industria es un sector de la actividad económica, es un sector de la industria que ha sido marginado. Hasta [hace un tiempo] nuestros bancos decían: ‹No, no podemos financiar un proyecto de defensa›. ¿¿Estás loco?? Así que sí, necesitamos que la Comisión preste más atención a la cuestión de la industria de defensa. Pero no simplifiquemos las palabras: una cosa es la industria de defensa y otra la defensa. ¿Industria de defensa? Con seguridad. La «defensa» por sí sola sería contraria a los Tratados.

[*reaccionando al orador anterior]*

…La Agencia de Defensa de la UE, que ya existe, no tenemos que esperar un año para crear una nueva estructura, ya ha creado [más de] 60 [contratos] marco para que los Estados miembros vayan a la industria y hagan pedidos de compra. la munición. Así que no inventes la rueda todos los días. Hay [más de] 60 marcos. Si quieres comprar más municiones para Ucrania, puedes usar una de ellas.

Si los Estados miembros que realmente están dispuestos a comprar más municiones para Ucrania tienen una manera de hacerlo de manera cooperativa, mediante adquisiciones conjuntas, todo el mundo habla de ello, ya existe, [más de] 60 [contratos] marco. para la compra conjunta a la industria y a los sitios industriales decir “tengo la capacidad, lo que me gusta son los pedidos”.

The President of Israel was here and said ‘Hamas is an existential question for us and the goad has not changed: we have to destroy Hamas’. There is a talk of a military operation in Rafah. How do you go about this?

A: Allow me to say first that maybe we should put into value what we have done for Ukraine. We can be self-critical. But please, please don’t dismiss what we have done for Ukraine. The unity has been remarkable. We mobilized the European Peace Facility for the first time in our history to provide arms to a country at war. We have to spend from our pockets - bilaterally and Member States - 28 billion of military support to Ukraine [so far] and civilian plus military it reaches 90 billion, more than the US. So, I am ready to be self-critical and I don’t want to say one country does more than the other, but my job is to try to make them work together and to put into value what we do.

And yes, we have to agree that we have been hesitating maybe too much, too many times. Two years ago, here, we were ready to give helmets. Now we are giving F-16s. But two years later. And every time we discussed about giving a new type of arms, someone was hesitating: 'No, no, no. Come on. We are not going to give them Leopards. It will be an escalation in the war'. In the end, we give Leopard. 'No, no, no. We are not going to give them Patriots. It will be an escalation of the war'. In the end we give them Patriots. 'No, no, no. We are not going to give them fighters [jets]'. And we are going to give fighters [jets].

Had we taken this decision quicker, maybe the war would have been different. But in spite of all, we have done a lot to support Ukraine. My only call is to do more and quicker, but not to dismiss what we have already done.

About Gaza. Look, Hamas is an idea, and you don't kill an idea. The only way you can kill an idea is to propose a better one. It is a bad idea, but it is an idea.

Many years ago, they said that they were going to destroy Hezbollah. Hezbollah is still there. So, I don't think that you can kill an idea. You have to provide an alternative which is better. And certainly, the alternative, the only alternative, is not to destroy Israel as Hamas wants to do, but to make Israel and Palestine live side by side in peace and common security.

And this will not be reached only by military means. I have been repeating it once and again: it will not be reached only by military means. And that's why I start my talks saying that we need an overall political solution to the conflict.

And how much do you worry about potentially this operation that will happen in Rafah, that, it seems, is next?

Emití un comunicado hace un par de días. Lamentablemente no pudimos alcanzar la unanimidad porque faltaba un país. Pero emití una declaración diciendo que pedimos encarecidamente a Israel que evite acciones militares contra una zona muy densamente poblada que es Rafah, donde 1,7 millones, casi 2 millones de personas están siendo empujadas contra un muro. Así que no creo que esto tenga que suceder. Pero mira, todo el mundo lo está pidiendo. Todos.

Preguntas diversas sobre la desinformación y sobre la Unión Europea dividida, interna y externamente, especialmente en política exterior y derechos humanos...

Quiero subrayar y seguiré diciendo que Europa tiene que aumentar su capacidad de defensa en el sentido más amplio de la palabra defensa. La defensa no es sólo militar. Es principalmente militar, pero no es sólo eso. Hay una lucha por la tierra y hay una lucha por el espíritu, por la mente del pueblo.

Y sí, hay una pelea sobre quién dice qué y quién le cree a quién. Y nosotros también estamos librando esta guerra. Hemos creado una estructura para desacreditar las mentiras difundidas por la propaganda rusa. Sabemos que existe algo que se llama "interferencia y manipulación extranjera". Luchamos contra ello y tenemos equipos dedicados a ello. Hemos asignado recursos y personas a África, a los Balcanes, donde la agresión rusa contra la mentalidad del pueblo es mucho más fuerte. Así que gracias por recordarlo. Lo estamos haciendo.

Somos perfectamente conscientes de que Rusia libra contra nosotros una guerra que no consiste únicamente en bombardear con obuses. Es una guerra de narrativas. Utilicé esta frase -estamos librando una guerra de narrativas- en el segundo mes de mi mandato. Y el que gane la guerra de las narrativas, estará mucho más preparado para ganar la otra guerra.

Y dentro de unos meses tendremos un proceso electoral en Europa y luego la opinión pública tendrá que saber y decidir cuánto apoyo quiere dar a Ucrania.

Derechos Humanos: sí, ciertamente. Somos uno de los mayores partidarios y defensores de los derechos humanos en todo el mundo. Nadie está haciendo más que nosotros. Quizás no me crean, pero díganme quién está haciendo más por defender los derechos humanos en el mundo. Nos pueden criticar por muchas cosas, no somos perfectos. Ciertamente desaprovechamos muchas ocasiones para expresarnos más cuando se violan los derechos humanos. Pero creo que la Unión Europea está haciendo mucho para apoyar la democracia y los derechos humanos en todo el mundo.

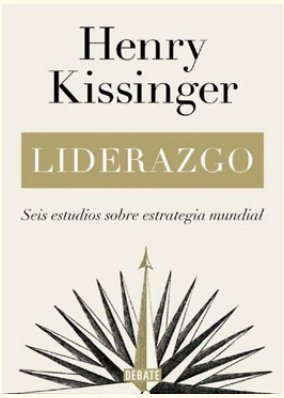

ACADEMIA NACIONAL DE ESTUDIOS POLITICOS Y ESTRATEGICOS
CHILE

RESEÑAS

LIDERAZGO. SEIS ESTUDIOS SOBRE ESTRATEGIA MUNDIAL*∞

GONZALO CARRASCO ASTUDILLO•

Henry Kissinger, reconocido mundialmente como un genio de la estrategia política, tuvo tal lucidez intelectual que pudo publicar su último libro a los 99 años, titulado "*Liderazgo. Seis estudios sobre estrategia mundial*" el 2022, editado en español por la Editorial Debate el 2023.



En 645 páginas la obra se inserta en la vida y la personalidad de seis líderes mundiales, cuyo liderazgo estratégico se desarrolló en escenarios de altísima complejidad, donde la presión y estrés fueron un obstáculo superado gracias al despliegue de una serie de virtudes humanas, fundamentalmente la "valentía" y la "fuerza de carácter". Los fascinantes líderes escogidos fueron: Konrad Adenauer, Charles de Gaulle, Richard Nixon, Anwar Sadat, Lee Kuan Yew y Margaret Thatcher.

Para Kissinger, el liderazgo es indispensable: "hay que tomar decisiones, ganarse la confianza, mantener las promesas, proponer una forma de avanzar" (p. 1) y para ello, un líder estratégico competente, debe moverse entre los ejes de "pasado y futuro" y "valores perdurables", todo desde una perspectiva realista del escenario político que se asoma a nuestra vista. En este sentido, el líder desempeña su trabajo siempre cercado por la escasez en una época con una determinada carga sociocultural que debe conocer bien, en una situación de competencia con otros actores (socios o adversarios) y todo con un flujo o rapidez de tanta intensidad, que no hay calma para cálculos precisos, debiéndose actuar conforme a intuiciones o meramente por medio de formulación de hipótesis.

Así, Kissinger nos inserta en las extremas condiciones del mundo político alemán post segunda guerra mundial, donde K. Adenauer tuvo que reconstruir a una Alemania, rendida incondicionalmente, luego del salvajismo de Hitler bajo una estrategia fundada en la humildad. Esa humildad, forjada sobre una profunda espiritualidad cristiana, le permitió poseer una visión estratégica con virtudes difíciles de ejercitar, como la "paciencia" en el restablecimiento de la legitimidad moral de Alemania frente a Europa y el mundo.

---

* Henry Kissinger, Santiago, Ed. Debate, 2023, Colección Sociedad, 645 páginas.

• Oficial de Ejército del Servicio de Justicia Militar. Licenciado en Ciencias Jurídicas, Abogado. LL.M Magíster en Derecho de la Pontificia Universidad Católica de Chile. Diplomado en Nuevas Tendencias en Contratos y Daños de la Pontificia Universidad Católica de Chile. Bachiller en Humanidades de la Universidad Andrés Bello. Alumno del Magíster en Seguridad, Defensa y Relaciones Internacionales de la Academia Nacional de Estudios Políticos y Estratégicos. gscarrasco@uc.cl ORCID: https://orcid.org/0009-0001-6941-2455

∞ Fecha de recepción: 261223 - Fecha de aceptación: 260624

Kissinger expone la manera en cómo, por medio de la humildad y la mirada a largo plazo, Adenauer pudo devolver la dignidad a Alemania con una renovada identidad nacional, aun frente a las dudas de muchos países relevantes como Francia. Señala el exsecretario de Estado de la Casa Blanca, que a Adenauer se le reconocía porque "[l]e preocupaban sobre todo las tendencias a largo plazo de Alemania, más que las cuestiones actuales" (p. 77). De esta manera, dejó un ejemplo de liderazgo y tradición que no se fundaba en una mera exultación transitoria, sino más bien en una capacidad de inspiración y visión en el tiempo.

Por otra parte, H. Kissinger nos muestra la "estrategia de la voluntad" de Charles De Gaulle, destacado político y militar francés, cuyo objetivo principal fue la restauración de la *grandeur* a Francia. Nos indica el autor que De Gaulle forjó una personalidad dominante, distante, apasionada, visionaria e inefablemente patriótica (p. 109) que se unían íntegramente en su estructura mental y su talentosa capacidad analítica. "La extraordinaria altura metafísica de la oratoria De Gaulle expresó su fe en la singularidad de su país" (p. 118), lo cual derivó en la principal característica de este militar como líder: buscar crear la realidad política mediante la exclusiva fuerza de voluntad, con razón y pasión.

Luego, es el turno de Richard Nixon, con quien Henry Kissinger tuvo una especial cercanía profesional. Los éxitos políticos de Nixon, así como sus complicaciones en el curso de la guerra con Vietnam del Norte y el desenlace del Watergate, se entrelazan con los de Kissinger, porque fue su asesor más confidente y muchas de las ideas de Nixon eran realmente las de Kissinger. En este punto, Raymond Aron fue profético cuando le advirtió que rezara por la supervivencia de Nixon, porque luego del presidente, irían por él.

En este punto Kissinger resalta la generosidad de Nixon con la invitación que le formuló para convertirse en el Asesor de Seguridad Nacional, el segundo nombramiento presidencial de mayor rango que no está sujeto a confirmación del Senado (p. 177). En efecto, ofrecer el cargo a un profesor universitario rompía con el pensamiento político convencional. En este punto, el autor y protagonista detalla el episodio del ofrecimiento, reconociendo su torpeza al pedirle al presidente "unos días para pensarlo" y la dura reprimenda que le dio Nelson Rockefeller (antiguo rival político de Nixon) al enterarse, quien lo instó a aceptar el trabajo sin condiciones y sin retraso, por solicitarlo el presidente de los Estados Unidos.

Luego llega el turno de analizar el liderazgo del militar y político egipcio Anwar Sadat, y su gran coraje por alcanzar la paz con Israel, aun cuando eso significó que en 1981 fuera asesinado en un desfile militar, por soldados que participaban del mismo, baleándolo hasta la muerte. Con clara asertividad proveniente de los rasgos propios de su personalidad, Kissinger señala que Sadat era una combinación quietista, pasando gran parte del tiempo reflexionando y orando antes que en el estrado político. Resulta interesante que esa tendencia a la soledad, que puede ser vista como una característica negativa, dotó a Sadat para tener perspicacia y un pensamiento independiente, desarrollando una gran capacidad de "paciencia estratégica", de importancia fundamental en las relaciones políticas internacionales, según el autor.

Continúa Kissinger con Lee Kuan Yew, primer ministro de Singapur, de quien Margaret Thatcher afirmó que "era uno de los hombres de Estado más dotados del siglo XX" (p. 354), y no estaba lejos de la realidad nos señala el autor del libro, ya que inició la épica tarea de transformar a Singapur, de su pobreza y contradicciones étnicas y culturales, a uno de los

países más ricos de Asia y el centro comercial del Sudeste Asiático. Por ello, Singapur "no era un país natural, sino uno hecho por los hombres" (p. 354).

Lee tenía grandes atributos de líder, probablemente marcados e influidos por el mundo de su infancia. En ese contexto, Kissinger nos cuenta que la familia Lee prosperó económicamente pero siempre dentro de una austeridad importante. "Se crio con su familia extendida –junto con siete primos- en la casa de su abuelo materno, donde sus padres compartían una sola habitación con sus cinco hijos" (p. 357). Esa temprana experiencia, sumado a su particular devoción filial, marcaron su frugalidad, su armonía y estabilidad. A los 12 años de edad ya destacaba por ser un estudiante inteligente, graduándose el primero de su clase en la escuela primaria (p. 358). Luego, ya como primer ministro, era respetado por líderes de Estado mucho más poderosos que el suyo, principalmente porque aportaba ideas esenciales con una gran capacidad de objetividad y lucidez.

Finalmente, el autor termina su recorrido con Margaret Thatcher, una líder que ubica como de aquellas que definen la época en que gobiernan, y así hay pocos. Como primera ministra del Reino Unido, devolvió un país revitalizado y optimista a fin de que no solo viviera de su glorioso pasado imperial y que a su llegada estaba en decadencia. Todo, gracias a su fortaleza personal, forjada por su condición de *outsider*: era la primera mujer en llegar al cargo, era del Partido Conservador y era de clase media (p. 401).

Afloraba su fortaleza, previamente a su vida política, en los primeros rechazos laborales que obtuvo como química, ya que en la evaluación interna de su postulación para trabajar en la Imperial Chemical Industries "se podía leer: Esta mujer es testaruda, obstinada y peligrosamente terca" (p. 411). Sin embargo, lo anterior demostraba más bien su gran vitalidad y compromiso en la manera de trabajar bien, con un carácter y determinación que constituían los primeros atisbos de la "Dama de Hierro".

Margaret Thatcher, según nos relata Kissinger, fundaba su liderazgo en un marco de soporte teórico o intelectual marcadamente diligente y profundo. Así, señala que "las ideas de Thatcher sobre política exterior se irían definiendo, gracias (…) a unos hábitos de estudio extraordinariamente diligentes –por ejemplo, leía y anotaba informes hasta bien entrada la noche- y a la costumbre de organizar, durante los fines de semana, seminarios con profesores universitarios e intelectuales sobre las tendencias a largo plazo" (p. 417).

Anticomunista férrea y conocedora de la tragedia moral, familiar y económica que trae a los países dicha ideología, defendió con fuerza el libre mercado. "Durante su mandato, los conservadores acabaron con los controles de divisa, eliminaron las comisiones comerciales fijas y abrieron el mercado de valores británico a los *traders* extranjeros, lo que se acabaría conociendo como el 'Bing Bang', lo cual a finales de la década de 1980 convirtió al país en un centro financiero internacional" (p. 422).

Cuando vinieron las complicaciones, donde los riesgos eran altos y la ambigüedad del entorno parecía no tener claridad cercana, Thatcher mantenía la calma y su fidelidad a sus convicciones, propio de los verdaderos líderes. Kissinger nos muestra cómo la "Dama de Hierro" nunca se retractó de su estrategia económica, aun cuando su tenacidad se mezclaba estratégicamente con la búsqueda de apoyo dentro del Partido Conservador. Asimismo, nos aclara cómo su especial dureza se encontraba unida indisolublemente con su patriotismo.

En definitiva, el libro “Liderazgo” de Henry Kissinger es una obra sorprendente en lucidez, considerando la edad del autor al ser escrito con 99 años de edad y que termina siendo su última obra poco antes de morir. Desde las virtudes de los distintos liderazgos que expone, se pueden sacar provechosos ejemplos para el propio ejercicio profesional, político y militar. Es lo que buscaba el profesor Kissinger en un mundo actual desorientado por falta de una visión moral y estratégica robusta: dejar una fuente de inspiración para que florezcan líderes con el carácter, el intelecto y la fortaleza necesaria a fin de encarar los desafíos políticos actuales.

A NUESTROS LECTORES Y COLABORADORES

NORMAS PARA LA PRESENTACIÓN DE ARTÍCULOS

1. Los trabajos que se presenten para ser publicados en la Revista deben ser: originales, inéditos y exclusivos, debiendo ser ingresados solamente a través de este portal, siguiendo los pasos que se señalan en http://www.politicayestrategia.cl/index.php/rpye/about/submissions#onlineSubmissions

   Su línea editorial está centrada en todos aquellos tópicos pertinentes y relevantes relativos a la Seguridad y Defensa con efectos a nivel nacional, regional y mundial, entre los que se encuentran asuntos políticos relacionados, amenazas a la paz y seguridad, pensamiento estratégico, transformaciones del escenario internacional, relaciones internacionales y derecho internacional.

   - Antes de subir el escrito a la plataforma de la revista, el autor está obligado a comprobar que su envío cumpla con todos los parámetros que se establecen para ello; sin perjuicio de lo anterior, una vez ingresado este es examinado nuevamente para verificar que se ha cumplido con aquella disposición.

   - En la eventualidad de que falte algún antecedente el autor será informado de aquello y su trabajo no será ingresado al Banco de Datos, como tampoco se dará inicio al proceso de evaluación de rigor hasta que la Dirección de la Revista cuente con la totalidad de los antecedentes establecidos.

   - Los autores deben incluir una declaración específica de que el artículo no se ha sometido a presentación para su evaluación y publicación en otras revistas simultáneamente, ni ha sido remitido para su difusión en otros medios (páginas web, libro electrónico, etc.).

   - En caso de haberse realizado alguna entrevista, se deberá adjuntar una copia del consentimiento Informado del entrevistado.

   - La revista no cobra tasa alguna por la revisión y publicación de los artículos. Por otra parte, los autores mantienen en todo momento los derechos sobre sus respectivos artículos.

   - Los trabajos pueden venir en idioma español o inglés, de todas maneras deben considerarse los resúmenes en ambos idiomas, además de portugués, independientemente del idioma del cuerpo del trabajo.

   - No se admiten artículos o traducciones de artículos ya publicados, salvo que la revista considere relevante hacerlo como reedición con fines de discusión, de antología o de divulgación con las autorizaciones correspondientes.

   - Tampoco es aceptable plagio alguno, ninguno de los datos incluidos en los trabajos presentados podrá ser plagiado, inventado, manipulado o distorsionado. La revista cuenta con el programa DOCODE que automatiza la detección del plagio en textos digitales, asegurando la originalidad de sus contenidos.

2. La revista es publicada semestralmente, siendo la primera edición en julio y la segunda en diciembre de cada año. Normalmente los trabajos se reciben hasta fines de mayo para la primera edición, y finales de octubre para la segunda edición.

3. Los conceptos, puntos de vista e ideas expuestos por los autores de los artículos que se publiquen serán de su exclusiva responsabilidad y no representan necesariamente el pensamiento de la Academia.

4. Con el objeto de lograr una mayor eficiencia y precisión en la publicación de los trabajos que se reciben, es conveniente que sus autores consideren las siguientes pautas:

   - Original en tamaño carta, con una extensión (aproximada) no mayor a 9.000 palabras y no menor a 7.000, en espacio simple, escritos en sistema Word, letra tamaño Arial Nº 12.

   - Todos los trabajos deben considerar en su parte introductoria lo siguiente: especificar su contextualización, señalar el problema de estudio, la o las preguntas directrices, el o los objetivos, la metodología y principales hallazgos (si es de investigación) o conclusiones preliminares si se trata de otra tipología, así como su enfoque. Debe ser claro, coherente y sucinto.

   - Genéricamente, los escritos deben considerar resumen, abstract, palabras claves (separadas por punto y coma), introducción, desarrollo, conclusiones, referencia bibliográficas y anexos si es del caso.

   - Las fotografías, gráficos y/o imágenes, dentro del texto, solo serán publicadas si su inclusión permite apoyar o clarificar el escrito para una mejor compresión de los lectores haciéndose presente que estas deben venir en blanco y negro por cuanto la revista, en su edición impresa, es en escala de grises. Para aquellos escritos que incluyan imágenes a color, los autores deben anexar el archivo de ambas versiones, en alta resolución, por cuanto la versión en línea de la revista se publica a color.

   - En el mismo sentido, se recomienda no usar imágenes o gráficos bajados de Internet porque su baja resolución impide una óptima impresión. Los autores deben respetar estrictamente los derechos de autor y fuentes de los cuadros y gráficos que se acompañen.

   - Todos los mapas deben ser publicables, es decir, sin restricciones de derechos de autor, ni condiciones que necesiten autorizaciones especiales. En el caso que incorporen mapas del territorio nacional de Chile la revista solicitará la correspondiente autorización de la Dirección de Límites y Fronteras (DIFROL) del Ministerio de Relaciones Exteriores de Chile, no responsabilizándose de los tiempos que este trámite demande respecto de la inclusión del artículo en el número previsto.

   - De ser imprescindible la inclusión de algunos de los elementos citados precedentemente, debe hacerse llegar el material en forma física con la finalidad de obtener una buena resolución de impresión, indicando la fuente de origen, con el propósito de no infringir la Ley de Propiedad Intelectual.

5. La Revista considera trabajos para cuatro secciones: Artículos, Estudios, Reseñas y Dossier.

   - **Artículos**

     Esta sección recoge trabajos de investigación y lo que se entiende habitualmente por monografía científica sobre los temas que se encuentren dentro de la línea editorial de la revista.

   - **Estudios**

     El estudio es un género literario que se caracteriza por permitir desarrollar un tema determinado de una manera libre y personal sin tener que ceñirse a una estructura rígida de redacción o documentarlo exhaustivamente.

   - **Reseñas**

     La reseña bibliográfica corresponde a un escrito breve que da cuenta del contenido de un libro que haya sido publicado y que responda a los temas señalados en la línea editorial de la revista. No debe sobrepasar de 3 páginas tamaño carta y deberá considerar, además, la siguiente información:

     - Título de la obra (si está en inglés, deberá incorporar traducción al español)
     - Autor o autores.
     - Lugar y año de edición.
     - Cantidad de páginas.
     - Imagen escaneada de la portada del libro, en alta resolución (se excluyen imágenes bajadas de Internet por su baja resolución e imposibilidad de una óptima impresión).

   - **Dossier**

     Lo entendemos aquí como documentos que desarrollan asuntos relevantes dentro del ámbito de la línea editorial de la revista y que contribuyen al conocimiento sobre seguridad y defensa.

6. Citas y referencias bibliográficas

   - Para las citas y referencias bibliográficas se debe usar el sistema ISO debiendo considerarse como referencia obligada el instructivo que se encuentra publicado en el sitio web de la Academia https://anepe.cl/wp-content/uploads/2020/10/NORMAS-ISO-ANEPE.pdf

   - La bibliografía debe necesariamente encontrarse actualizada respecto del estado del problema en cuestión, ser relevante, pertinente y debe considerar, idealmente, publicaciones indexadas en bases de datos o repositorios más utilizados como, por ejemplo, Scopus, Wos o Scielo.

- Adjuntar resumen (abstract) del tema en español, inglés y portugués, de una extensión máxima de 15 líneas. Además, deben incluir palabras clave para facilitar que los artículos sean localizados en los motores de búsqueda de Internet.

- Las palabras clave, al igual que el título, deben venir en español, inglés y portugués y separadas por punto y coma (semicolon).

- En atención a que la revista se encuentra en línea, y de acuerdo a las normas ISSN para este efecto cuando se cite o referencie a ella debe colocarse "Polít. estrateg. (En línea)".

- Adjuntar breve currículum, principalmente títulos y grados académicos, institución actual de trabajo, país, dirección de contacto (e-mail), teléfono para efectos de que se puedan realizar los contactos entre la editorial y los autores y, finalmente, incluir el ORCID para lo cual se recomienda obtenerlo en https://orcid.org/

7. Selección de los trabajos

- Cada artículo es sometido a revisión de un cuerpo de consejeros, tanto nacionales como extranjeros, de reconocida experiencia en cada uno de los temas que la revista aborda bajo el concepto de "referato ciego". Sus respectivos informes son remitidos al Consejo Editorial, cuyos integrantes deciden la publicación o no de los trabajos. Los escritos que no sean aprobados por el consejo de la revista serán devueltos a sus autores quedando a su total disposición.

- También el Consejo Editorial podrá formular observaciones para que los artículos sean revisados y se ajusten a la política editorial de la Revista.

- Otras informaciones de detalle se deben consultar al Correo Electrónico rpye@anepe.cl

Envío del manuscrito

Los manuscritos deben ser ingresados directamente por sus autores a la plataforma electrónica http://www.politicayestrategia.cl, quien emite en forma automática el acuse de recibo de envío, siguiendo las instrucciones que da el sistema "*Open Journal System* (OJS) de acuerdo a lo siguiente:

- Para envío de artículos ingresar al link:

  https://www.politicayestrategia.cl/index.php/rpye/about/submissions

- Si no es usuario, ingresar al link que se indica para tener acceso al Manual del Autor:

  https://www.politicayestrategia.cl/index.php/rpye/index

COMPROMISO ÉTICO

La política de la revista se guiará por el compromiso ético de la investigación científica y sigue las normas éticas presentadas en el *Best Practice Guidelines for Journal Editors y el International Standards for Editors and Authors* publicado por el Committee on Publication Ethics – COPE.

De la revista

El proceso editorial se atendrá a los principios éticos y científicos.

No se admiten artículos ya publicados, traducciones de artículos ya publicados, ni plagios. Ninguno de los datos incluidos en los trabajos presentados habrá sido plagiado, inventado, manipulado o distorsionado.

En el momento en que el artículo sea aceptado por los órganos competentes de la revista, el autor o autores deberán rellenar un formulario específico donde constarán las condiciones de copyright de la revista.

La revista no cobrará por la publicación de artículos, ni se pagará a los autores por los mismos.

Del Consejo Editorial

El Consejo Editorial velará por el cumplimiento de los principios de ética editorial.

La opinión de los miembros de los consejos de la revista no tiene que coincidir necesariamente con las opiniones expuestas en los textos publicados, que son responsabilidad exclusiva de sus autores.

El Consejo Editorial analizará todas las contribuciones, podrá rechazar un artículo, sin necesidad de evaluarlo, si considera que no se adapta a las normas o no se adecua al perfil de contenidos de la publicación. Excepto en esos casos, la decisión de publicar o no un trabajo se basará en el dictamen de los revisores externos a la entidad editora, empleándose el sistema de «doble ciego».

Las sugerencias de los revisores serán enviadas a los autores para que, en caso necesario, realicen las modificaciones pertinentes.

Se informará al autor sobre la aceptación o rechazo de su contribución en un plazo máximo de seis meses, excepto cuando se hayan exigido modificaciones que alarguen el proceso de evaluación.

De los autores

Los trabajos serán originales e inéditos. Al enviar el artículo los autores deben incluir una declaración específica de que el artículo no se ha sometido a presentación para su evaluación y publicación en otras revistas simultáneamente o con anterioridad, ni ha sido remitido para su difusión en otros medios (páginas web, libro electrónico, etc.).

Los datos y teorías originales se distinguirán claramente de los ya publicados, que se identificarán citando las fuentes originales, así como otros trabajos previamente publicados.

Igualmente se citarán adecuadamente la procedencia de las figuras, tablas, datos, fotografías, etc., previamente publicados, y se aportarán los permisos necesarios para su reproducción en cualquier soporte.

Todas las personas que firmen los trabajos deben haber participado en la elaboración y revisión del mismo, y estar de acuerdo con su publicación. Así mismo se respetarán los criterios de autoría científica, sin excluir a ningún responsable del trabajo.

La revista declina cualquier responsabilidad sobre posibles conflictos derivados de la autoría de los trabajos que se publican en la misma, provocados por el incumplimiento de sus normas.

Los autores se comprometen a que en caso de detectar cualquier error en el artículo, antes o después de su publicación, alertarán inmediatamente a la Dirección de la Revista y aportarán, en caso necesario, la corrección de los errores detectados. Si se ha producido después de la publicación, la revista publicará así mismo correcciones, aclaraciones, rectificaciones y disculpas cuando sea necesario.

Los autores aceptan someter sus trabajos a un proceso de revisión anónima por pares.

Los artículos podrán ser retirados en cualquier momento del proceso de evaluación por los autores que estén en desacuerdo con las decisiones adoptadas en cualquiera de sus instancias de evaluación y resolución, o por otros motivos que estos manifiesten.

De los revisores

Los revisores tratarán el artículo de forma confidencial.

En el caso de que exista cualquier incompatibilidad o conflicto de intereses, los revisores se abstendrán de la evaluación y lo comunicarán a la secretaría de redacción. Esta exigencia debe ser prioritaria para los evaluadores, ya que no parece necesario subrayar que dada la especificidad de algunos de los campos de la revista, el número de especialistas que pueden existir es muy escaso, por lo que pese a los esfuerzos de la revista para conservar el anonimato, los evaluadores pueden llegar a identificar con cierta seguridad a los autores.

Esa sospecha no inhabilita para la evaluación, pero sí la incompatibilidad o conflicto de intereses con el hipotético autor.

La revisión será objetiva y constructiva y, teniendo en cuenta lo anterior, la exigencia de neutralidad debe considerarse una prioridad absoluta.

Los revisores deben tener en cuenta que no se admiten artículos ya publicados, traducciones de artículos ya publicados, ni plagios.

Los revisores se comprometen a indicar bibliografía interesante o novedosa.

Los revisores se comprometen a orientar al autor acerca de trabajos aún no publicados y de líneas de investigación en desarrollo que puedan afectar al texto.

LIBROS COLECCIÓN DE INVESTIGACIONES ANEPE

LIBROS COLECCIÓN DE INVESTIGACIONES ANEPE

Principio	Definición
Nº 1	**Textos Básicos del Derecho Humanitario Bélico.** Eugenio Pérez de Francisco y Arturo Contreras Polgati Pp. 375 - Año 2002
Nº 2	**La Comunidad de Defensa en Chile.** Francisco Le Dantec Gallardo y Karina Doña Molina Pp. 101 – Año 2002
Nº 3	**Crisis Internacionales en Sudamérica: Teoría y Análisis.** Aquiles Gallardo Puelma Pp. 367 – Año 2003
Nº 4	**Seguridad Humana y Seguridad Nacional: Relación conceptual y práctica.** Claudia F. Fuentes Julio Pp. 93 – Año 2004
Nº 5	**Una estructura para la asesoría en el manejo de crisis internacionales: caso nacional.** Juan Carlos Verdugo Muñoz.- Pp. 101 – Año 2004
Nº 6	**La disuasión convencional, conceptos y vigencia.** Marcos Bustos Carrasco y Pablo Rodríguez Márquez Pp. 147 – Año 2004
Nº 7	**La Corte Penal Internacional y las Operaciones de paz: competencias y alcances.** Astrid Espaliat Larson Pp. 95 – Año 2004
Nº 8	**Operaciones de Paz: tres visiones fundadas.** Cristian Le Dantec Gallardo - Guillermo Abarca Ugarte - Agustín Toro Dávila - Juan Gmo. Toro Dávila y Martín Pérez Le-Fort Pp. 439 – Año 2005
Nº 9	**Alcances y realidades de lo Político-Estratégico.** Cátedra de Seguridad y Defensa de la ANEPE Pp. 104 – Año 2005
Nº 10	**La protección de los recursos hídricos en el Cono Sur de América. Un imperativo de seguridad para el siglo XX".** Pablo Rodríguez Márquez y Mario L. Puig Morales Pp. 200 – Año 2005
Nº 11	**Bolivia 2003. Percepciones de la crisis en la prensa chilena y su impacto en la seguridad subregional y relaciones bilaterales.** Iván Witker Barra Pp. 172 – Año 2005

Nº 12	**Hacia un sistema de seguridad subregional en el Mercosur ampliado: rol de la globalización como factor de viabilidad y agente estructurador.** Hernán L. Villagrán Naranjo Pp. 81 – Año 2005
Nº 13	**La estrategia total. Una visión crítica.** Galo Eidelstein Silber Pp. 298 – Año 2006
Nº 14	**La seguridad internacional en el siglo XXI, más allá de Westfalia y Clausewitz.** Mariano César Bartolomé Inglese Pp. 358 – Año 2006
Nº 15	**Chile y las Operaciones de Paz. Estudio comparado de la política exterior de los tres gobiernos concertacionistas. De la reinserción internacional a la participación en Haití.** Paulina Le Dantec Valenzuela Pp. 175 – Año 2006
Nº 16	**La cooperación en el ámbito de la seguridad en el comercio en la región Asia Pacífico: la iniciativa STAR del Foro APEC.** Eduardo Silva Besa - Cristóbal Quiroz Costa e Ignacio Morandé Montt Pp. 130 – Año 2006
Nº 17	**Amigos y vecinos en la costa del Pacífico. Luces y sombras de una relación.** Cristian Leyton Salas Pp. 263 – Año 2007
Nº 18	**Chile y sus intereses en la Antártica. Opciones políticas y de seguridad frente a la escasez de recursos hídricos.** Pablo Rodríguez Márquez y Mario L. Puig Morales Pp. 109 – Año 2007
Nº 19	**El problema de la guerra y la paz en Kant.** Carlos Molina Johnson Pp. 110 – Año 2007
Nº 20	**El agua como factor estratégico en la relación entre Chile y los países vecinos.** Cristián Faundes Sánchez Pp. 370 – Año 2008
Nº 21	**Los aportes del Mercosur a la seguridad subregional. Un enfoque desde la Seguridad y Defensa Nacional de Chile.** Jorge Riquelme Rivera Pp. 180 – Año 2009
Nº 22	**Los Libros de la Defensa Nacional de Chile 1997-2002 como instrumentos de Política Pública.** Juan A. Fuentes Vera Pp. 410 – Año 2009
Nº 23	**La Guerra. Su Conducción Política y Estratégica. (Re-edición)** Manuel Montt Martínez (Autor fallecido) Pp. 366 – Año 2010

Nº 24	**La Fuerza de Paz “Cruz del Sur”. Instrumento del multilateralismo chileno-argentino.** General de División Cristián Le Dantec Gallardo Pp. 232 – Año 2010
Nº 25	**Crisis Internacionales** Rodolfo Ortega Prado Pp. 280 – Año 2011
Nº 26	**La Conducción de la Defensa Nacional: Historia, presente y futuro.** Carlos Molina Johnson - Miguel Navarro Meza - Luis Rothkegel Santiago - Julio Soto Silva Pp. 184 – Año 2012
Nº 27	**Desafíos nacionales en un contexto internacional complejo.** Departamento de Estudios Políticos y Estratégicos de la ANEPE Pp. 349 – Año 2013
Nº 28	**Prevención de conflictos. Unión Europea – Latinoamérica.** Rodolfo Ortega Prado (Chile) – Luis de la Corte Ibáñez (España) - Fernando Lista Blanco (España) Pp. 363 – Año 2013
Nº 29	**La amenaza terrorista para la seguridad internacional. Estudio comparado de casos de toma de rehenes.** Ariel Álvarez Rubio – Alejandro Salas Maturana Pp. 345 – Año 2013
Nº 30	**Amenazas multidimensionales: Una realidad en Suramérica.** Carlos Ojeda Bennett Pp. 121 – Año 2013
Nº 31	**La Antártica como escenario de cooperación: Oportunidades para afianzar el statu quo.** CDG (BA) Miguel Figueroa Ibarra Pp. 116 – Año 2014
Nº 32	**El sistema de planificación de la Defensa: Requerimientos y desafíos para la gobernabilidad del sector.** Gonzalo Álvarez Fuentes Pp. 83 – Año 2014
Nº 33	**Las Maras: una amenaza a la Seguridad Nacional** Ricardo Rodríguez Arriagada. Pp. 153 – Año 2014
Nº 34	**Asia Pacífico. Nuevos enfoques de Seguridad y Defensa.** Departamento de Estudios Políticos y Estratégicos de la ANEPE Pp. 278 – Año 2015
Nº 35	**La Defensa en perspectiva académica: Historia y proyección.** Julio Soto Silva – Miguel Navarro Meza – Alejandro Salas Maturana Pp. 200 – Año 2015
Nº 36	**Mujer, paz y seguridad: implementación de la Resolución 1325 del Consejo de Seguridad en Chile.** Maricel Sauterel Gajardo Pp. 166 – Año 2015

Nº 37	**Gobernabilidad, desarrollo y seguridad en las zonas extremas de Chile.** Loreto Correa Vera – Alejandro Salas Maturana Pp. 326 – Año 2015
Nº 38	**Responsabilidad de Proteger. Deber-Poder de la comunidad internacional y limitación de la soberanía.** José Héctor Marinello Federici Pp. 135 – Año 2016
Nº 39	**Desafíos de la Seguridad y Defensa en el mundo contemporáneo.** Unidad Académica – Departamento Docente ANEPE Pp. 333 – Año 2016
Nº 40	**Estrategias para combatir las amenazas multidimensionales en la Región.** Aracely Banegas Alfaro Pp. 118 – Año 2017
Nº 41	**Elementos Políticos y Estratégicos en las decisiones de políticas públicas.** Cuerpo Académico ANEPE Pp. 362 – Año 2018
Nº 42	**El tráfico ilícito de migrantes y la trata de personas: Comparación y evaluación de las políticas en Chile.** Francisca Barros Sánchez Pp. 182 – Año 2018
Nº 43	**Procesos Migratorios en Chile: Una mirada histórica-normativa.** Guillermo Bravo Acevedo – Carmen Norambuena Carrasco Pp. 152 – Año 2018
Nº 44	**Estudio comparado del Sistema Preventivo del Lavado de Activos implementado en: Perú, Chile, Colombia y México entre 2000-2016.** Cristian Rosales Morales Pp. 145 – Año 2018
Nº 45	**Antecedentes para el debate acerca de una Estrategia de Seguridad Nacional.** Cuerpo Académico ANEPE Pp. 230 – Año 2019
Nº 46	**Chile y Bolivia: Distanciamiento, crisis y aproximación.** Loreto Correa Vera Pp. 293 – Año 2020
Nº 47	**Fuerzas Armadas y Constitución ¿De qué se trata? (Edición Especial)** C.I.E.E. ANEPE. Pp. 137 – Año 2021
Nº 48	**Chile y su ámbito vecinal: reflexiones sobre Política Exterior** Alejandro Salas Maturana (ed.) Pp. 166 –Año 2021
Nº 49	**Construyendo futuro: Chile y Perú en el siglo XXI** Jorge Gatica Bórquez Pp. 180 –Año 2022
Nº 50	**Plataforma Continental y Antártica Chilena. Antecedentes históricos, geopolítica y recursos naturales** Karen I. Manzano Iturra – Diego I. Jiménez Cabrera Pp. 118 – Año 2022

Academia Nacional de Estudios
Políticos y Estratégicos

Eliodoro Yañez 2760 - Providencia - Santiago
Teléfono: (56) 2598 10 00 Fax: (56) 2598 10 43
Página web: www.politicayestrategia.cl - www.anepe.cl
Correo electrónico: rpye@anepe.cl