CARI /

ASUNTOS GLOBALES

Número 2
Diciembre 2025

América Latina

Actores no estatales, nuevas tecnologías y conflictos posmodernos: desafíos estratégicos para América Latina

Juan Belikow

Actores no estatales, nuevas tecnologías y conflictos posmodernos: desafíos estratégicos para América Latina

Juan Belikow

Licenciado en Ciencia Política por la Universidad de Buenos Aires y doctor en Ciencia Política por la Universidad de Belgrano. Miembro Consejero del CARI. Consultor de la Organización de las Naciones Unidas, el Banco Mundial, el Banco Interamericano del Desarrollo, la Organización de Estados Americanos y la Organización para la Seguridad y la Cooperación de Europa. Es profesor en universidades de la Argentina y el exterior. Correo de contacto: Jbelikow@hotmail.com

1. Introducción

América Latina se enfrenta a un panorama de seguridad y gobernanza radicalmente transformado por la irrupción de actores no estatales tecnológicamente empoderados. Mientras las guerras contemporáneas —como las de Ucrania e Israel-Palestina— introducen nuevas lógicas de confrontación basadas en tecnología, desmaterialización de los ataques y participación encubierta de múltiples actores, la región latinoamericana, aun sin ser epicentro de estos conflictos, comienza a experimentar sus efectos colaterales. Detrás de la fachada de guerras entre Estados, lo que se perfila es una creciente participación de operadores no estatales en funciones tradicionalmente estatales: defensa, inteligencia, logística, propaganda, manipulación cognitiva y sabotaje, entre otras.

Este artículo explora la intersección entre actores no estatales, nuevas tecnologías y conflictos posmodernos, destacando cómo estas dinámicas reconfiguran la seguridad, la política exterior y el desarrollo socioeconómico en América Latina. Se parte de la hipótesis de que el creciente protagonismo de actores informales y privados, dotados de recursos técnicos y financieros cada vez más sofisticados, representa una amenaza directa a la gobernanza democrática, el monopolio estatal del uso de la fuerza y la estabilidad regional. Asimismo, se sostiene que la región aún no ha internalizado completamente los riesgos que implican estas nuevas formas de poder asimétrico.

2. Marco conceptual: las generaciones de la guerra y el rol emergente de los actores no estatales

La evolución de los conflictos armados a lo largo de la historia ha dado lugar a distintas "generaciones" de guerra, cada una definida por sus lógicas estratégicas, tecnologías predominantes y actores involucrados (Lind, Nightengale, Schmitt, Sutton y Wilson, 1989; Hammes, 2004). Comprender esta evolución resulta crucial para dimensionar la transformación actual del panorama de seguridad global.

- Guerra de cuarta generación (4GW): caracterizada por la erosión del monopolio estatal de la violencia, la aparición de actores no estatales armados (guerrillas, insurgencias, redes criminales) y la fusión entre guerra y política. Aquí se desdibujan las líneas entre combatientes y civiles, y el control narrativo se vuelve clave (Lind *et al.*, 1989).

- Guerra de quinta generación (5GW): incorpora elementos de manipulación informativa, guerra psicológica, desinformación y operaciones en el ciberespacio. Las percepciones sociales se convierten en objetivos militares, y los ataques pueden ser no cinéticos, pero son altamente desestabilizadores (Reed, 2008).

- Guerra de sexta generación (6GW): proyecta un escenario futuro donde los conflictos estarán dominados por sistemas autónomos, inteligencia artificial, armas hipersónicas y guerra multidominio. La automatización del combate y la intervención de operadores sin identificación estatal son parte constitutiva del conflicto (Hammes, 2004).

En estas tres fases coexisten actores estatales y no estatales; estos últimos son cada vez más relevantes. Algunos operan al servicio de los Estados; otros, por cuenta propia; y muchos, en alianzas informales, grises o directamente criminales. Las tecnologías de uso dual (civil y militar), como drones, IA, criptomonedas y sistemas de vigilancia, han permitido que grupos criminales, terroristas, mercenarios, corporaciones o individuos altamente capacitados accedan a capacidades antes reservadas a los ejércitos nacionales.

Esta tendencia tiene implicaciones profundas para América Latina, donde el crimen organizado, las redes de trata, los carteles del narcotráfico y otras estructuras no estatales ya ejercen control sobre territorios, rutas, economías y poblaciones enteras, y muchas veces poseen mayores capacidades operativas que las fuerzas estatales locales.

3. El rol de los actores no estatales tecnológicamente empoderados

En el contexto de los conflictos contemporáneos, los actores no estatales ya no son elementos marginales o simplemente reactivos. Han emergido como protagonistas activos y, en algunos casos, decisivos en la evolución táctica y estratégica de la guerra posmoderna. Esta categoría incluye una amplia gama de operadores: desde grupos criminales con estructuras paramilitares, empresas privadas de seguridad, redes de *hackers* mercenarios y emprendedores tecnológicos hasta comunidades

ideológicas movilizadas digitalmente. Estos actores combinan acceso a tecnologías de uso dual —cuyo origen puede ser civil o militar— con redes globales de conocimiento y financiamiento.

A diferencia de generaciones anteriores, estos operadores no requieren de grandes arsenales ni de estructuras burocráticas para proyectar poder. Un pequeño equipo con acceso a inteligencia artificial, redes sociales, herramientas de vigilancia digital y criptofinanzas puede desestabilizar un territorio, sabotear infraestructuras críticas o ejecutar operaciones de espionaje a gran escala. Casos como el uso de drones explosivos de fabricación artesanal por parte de Ucrania dentro del territorio ruso, o la adquisición y empleo del *software* de espionaje Pegasus, o la *weaponización* de *pagers* por actores estatales y no estatales fuera de marcos legales ilustran cómo estas capacidades se han descentralizado y democratizado peligrosamente.

Lo que agrava el fenómeno es que muchos de estos actores no buscan integrarse al aparato estatal ni subordinarse a él: encuentran mayores márgenes de acción, mejores incentivos económicos y menos restricciones éticas o legales fuera del Estado. La tercerización de funciones críticas —como la ciberseguridad, la inteligencia, la propaganda o incluso la coerción armada— por parte de algunos Gobiernos ha contribuido a consolidar este fenómeno. Como resultado, asistimos a una fragmentación de la autoridad y del control sobre el uso de la fuerza y la información, e incluso del conocimiento técnico especializado.

Una pregunta clave, aún sin respuesta satisfactoria, se impone: ¿qué ocurrirá con estos actores cuando cesen los conflictos que hoy justifican su existencia y financiamiento? ¿Qué harán esos programadores, ingenieros, pilotos de drones, analistas de OSINT (por las siglas de *Open Source Intelligence*: "inteligencia de fuentes abiertas") o expertos en ciberdefensa, que adquirieron experiencia de combate, entrenamiento avanzado y acceso privilegiado a tecnologías punta? La historia sugiere que muchos de ellos —desvinculados de sus empleadores estatales o corporativos— podrían canalizar su *expertise* hacia actividades criminales, insurgentes o disruptivas. Tal como ocurrió con antiguos combatientes de conflictos del siglo XX, que nutrieron las filas del crimen organizado o del terrorismo, hoy corremos el riesgo de que operadores tecnológicamente empoderados terminen integrando estructuras criminales transnacionales o mercados ilegales digitales y tecnológicos.

Ya existen señales de esta deriva: redes de narcotráfico en América Latina emplean tecnología de reconocimiento facial, drones, semisumergibles, criptografía y herramientas de análisis predictivo para optimizar sus operaciones y evitar a las autoridades; bandas de secuestradores acceden a plataformas de rastreo geolocalizado y drones para identificar objetivos; mercados oscuros en la *darknet* ofrecen armas, drogas, *software* de espionaje, servicios de sicariato, acceso a bases de datos y servicios de ataque DDoS (o ataque de denegación de servicio) por encargo. A esto se suman los casos documentados de expertos en ciberseguridad desvinculados de agencias públicas que luego ofrecieron sus servicios en mercados grises o directamente ilegales.

Como ha advertido el World Economic Forum (2023), la "*weaponización* del talento" es una de las tendencias de riesgo más relevantes en los próximos años: indivi-

duos con capacidades técnicas de elite actuando fuera de marcos legales, muchas veces bajo el anonimato o al amparo de estructuras corporativas o estatales que los utilizan como herramientas de poder indirecto. El caso de los desarrolladores del *software* Pegasus involucrados en operaciones no autorizadas es solo uno de muchos ejemplos posibles.

En este nuevo ecosistema, la distinción entre guerra, crimen y comercio se diluye. Los actores no estatales tecnológicamente empoderados se mueven con fluidez entre esos mundos. Esta fluidez, combinada con la desregulación de los mercados digitales, la opacidad de las criptofinanzas, la proliferación de tecnologías de bajo costo y la incapacidad de muchos Estados para rastrear operaciones complejas, configura un escenario de alta inestabilidad sistémica. América Latina, por sus brechas institucionales, sus redes de criminalidad organizada transnacional y su débil gobernanza tecnológica, se convierte en un terreno fértil para que estos operadores encuentren refugio, mercado y oportunidades.

Por ello, el análisis del rol de los actores no estatales tecnológicamente empoderados no debe limitarse al campo de la seguridad ciudadana o de la batalla convencional ni al plano de la seguridad digital. Debe ser abordado como un fenómeno estructural que transforma la naturaleza del poder, la autoridad y la gobernabilidad en el siglo XXI. El reto no solo consiste en contenerlos, sino en comprender sus lógicas, sus motivaciones y sus trayectorias futuras. El verdadero riesgo no es solo su existencia, sino además su capacidad para reconfigurar —desde la sombra— el equilibrio de poder global y regional.

4. Consecuencias estratégicas para la gobernanza y la seguridad regional

La consolidación de actores no estatales tecnológicamente empoderados y su penetración en ámbitos tradicionalmente reservados al Estado han generado efectos disruptivos sobre la gobernanza y la seguridad en América Latina. Este fenómeno, impulsado por la disponibilidad de tecnologías de uso dual y la fragmentación del monopolio estatal del poder, ha erosionado el control soberano sobre funciones críticas, como la seguridad, la información y la gestión del conocimiento.

Una de las consecuencias más preocupantes es la erosión del poder estatal y la captura institucional. En diversas regiones del continente, especialmente en zonas periféricas o fronterizas, la presencia efectiva del Estado ha sido reemplazada por organizaciones criminales que controlan territorios, ofrecen protección a comunidades locales y regulan economías ilegales. Al incorporar tecnologías avanzadas —como drones, armas fabricadas con impresoras 3D, inteligencia artificial, criptomonedas y vigilancia biométrica—, estas organizaciones fortalecen su capacidad de ejercer violencia, recolectar información, intimidar y manipular la percepción pública. En algunos casos, su poder técnico y operativo supera al de las fuerzas públicas, lo que genera un entorno de gobernanza paralela y cooptación institucional.

Paralelamente, se observa una fragmentación y privatización de la seguridad. Ante la incapacidad de los Estados para proveer protección eficaz, las élites económicas recurren a empresas de seguridad privada, que despliegan sus propias redes de vigilancia, análisis de riesgos y operaciones de defensa cibernética. Esta tendencia

refuerza la desigualdad: mientras los sectores más acomodados acceden a soluciones de protección de alta tecnología, las poblaciones vulnerables quedan expuestas a la violencia organizada o a la represión informal. En muchos casos, estas empresas operan sin una regulación adecuada, lo que dificulta la rendición de cuentas y propicia la tercerización de funciones sensibles del Estado.

Otra dimensión crítica es la vulnerabilidad cognitiva de las sociedades latinoamericanas. En línea con las características de la guerra de quinta generación, los actores no estatales y estatales han desplegado campañas de desinformación, manipulación electoral y polarización social utilizando redes sociales, inteligencia artificial generativa (como los *deepfakes*), bots automatizados y técnicas de *microtargeting*. Esta manipulación informativa socava la cohesión social, genera desconfianza institucional y debilita los procesos democráticos. En muchos países de la región, esta guerra cognitiva se desarrolla sin una estrategia estatal de respuesta y con una ciudadanía expuesta a narrativas tóxicas e injerencias externas.

Simultáneamente, el crimen organizado transnacional ha modernizado su estructura operativa. Lejos de ser estructuras rudimentarias, los carteles y redes ilícitas funcionan como verdaderas corporaciones criminales: contratan expertos en ciberseguridad, utilizan plataformas de mensajería encriptada, emplean criptomonedas para el lavado de activos y explotan el *big data* para identificar rutas, patrones de consumo y objetivos vulnerables. Este proceso de "corporativización criminal" hace que, para los Estados, sea cada vez más difícil combatirlos con herramientas tradicionales, pues requieren capacidades técnico-operativas y normativas de alto nivel que muchos países latinoamericanos aún no poseen.

Además, se produce una asimetría estratégica creciente. A las diferencias entre actores estatales y no estatales se suman las asimetrías entre Estados. Mientras algunos países desarrollan capacidades cibernéticas ofensivas y defensivas, otros apenas están diseñando estrategias de ciberseguridad. Esta brecha regional complica la cooperación intergubernamental, obstaculiza la construcción de respuestas colectivas y aumenta la exposición de los eslabones más débiles a ser utilizados como plataformas logísticas o financieras por redes criminales globales.

Finalmente, la presencia de estos actores no estatales en el espacio digital y operativo debilita la arquitectura internacional de seguridad. Instrumentos como la Convención de Palermo, las resoluciones de la OEA en materia de ciberseguridad y las normas del GAFILAT sobre delitos financieros se ven desbordados por la velocidad de innovación y la opacidad operativa de estos actores. Muchas veces, las redes criminales y sus aliados superan en agilidad a las agencias estatales, burlan los controles de transacciones internacionales y operan a través de jurisdicciones laxas o paraísos digitales.

En conclusión, la aparición y consolidación de actores no estatales tecnológicamente empoderados ha alterado profundamente la lógica de la seguridad y la gobernanza en América Latina. Ya no se trata solo de amenazas externas o desafíos clásicos a la soberanía: lo que está en juego es la capacidad de los Estados para regular, proteger y gobernar en un entorno donde las reglas del juego han cambiado

y los jugadores operan en múltiples dominios, muchas veces invisibles y siempre dinámicos.

5. Propuestas de respuesta estratégica para América Latina

Frente al creciente protagonismo de actores no estatales tecnológicamente empoderados, las amenazas híbridas y la disolución de los límites entre lo civil y lo militar, América Latina requiere respuestas estratégicas sistémicas, multidisciplinarias y adaptativas. La región no puede enfrentar desafíos posmodernos con herramientas del siglo pasado. Este capítulo propone una serie de líneas de acción estratégicas que abarcan lo normativo, lo institucional, lo operativo y lo cultural, con énfasis en la prevención, la resiliencia y la innovación.

5.1. Fortalecimiento normativo y doctrinario

Uno de los primeros pasos consiste en actualizar y armonizar los marcos legales nacionales y regionales para hacer frente a los desafíos que plantea el uso dual de tecnologías y la tercerización de funciones estatales críticas. Se requieren leyes claras sobre los siguientes puntos:

- Gobernanza de datos sensibles y algoritmos de decisión automatizada.
- Regulación del uso de drones y vehículos autónomos en seguridad y defensa.
- Tercerización de servicios de ciberseguridad e inteligencia privada.
- Supervisión de herramientas de vigilancia, interceptación y reconocimiento facial.

Asimismo, se recomienda alinear las normativas nacionales con los estándares propuestos por la Organización para la Cooperación y el Desarrollo Económico (OCDE) sobre gobernanza digital, protección de infraestructura crítica, integridad institucional y competencia leal (Organización para la Cooperación y el Desarrollo Económico, 2021), y con las recomendaciones de GAFILAT sobre trazabilidad financiera, transparencia de beneficiarios finales, monitoreo de transacciones sospechosas y regulación de criptomonedas (FMI y GAFILAT, 2023). Además, la adopción del Programa Interamericano de Ciberseguridad de la OEA (Organización de los Estados Americanos, 2022) puede fortalecer las capacidades regionales para la defensa cibernética.

5.2. Profesionalización e integración institucional

La respuesta a amenazas híbridas no puede quedar fragmentada. La región debe avanzar hacia la creación de estructuras interagenciales de respuesta integral que articulen defensa, seguridad interior, inteligencia civil y financiera y ciberdefensa. Esto implica:

- Crear centros nacionales de fusión de inteligencia y análisis multidominio.

- Fortalecer las capacidades del poder judicial y los ministerios públicos en delitos tecnológicos y complejos.
- Capacitar a las fuerzas armadas y policiales en tecnologías emergentes (IA, *blockchain*, IoT, etc.).
- Establecer comandos conjuntos de seguridad multidimensional ante crisis híbridas.
- Incorporar protocolos de interoperabilidad entre agencias públicas y actores privados.

Esta integración requiere superar la tradicional compartimentación institucional y la competencia entre agencias, promoviendo, en cambio, una cultura de cooperación y complementariedad.

5.3. Inversión en innovación y capacidades tecnológicas soberanas

La dependencia tecnológica de proveedores externos y el rezago en capacidades autóctonas aumentan la vulnerabilidad regional. América Latina debe invertir en los siguientes elementos:

- Ecosistemas de innovación público-privada en tecnologías estratégicas.
- Centros de desarrollo de IA, ciberseguridad, criptografía e inteligencia automatizada.
- Plataformas regionales de intercambio de alertas tempranas y datos de amenazas.
- Formación de profesionales con dominio técnico-cognitivo en seguridad digital.

Un ejemplo para seguir es el impulso a *startups* de seguridad digital latinoamericanas, en cooperación con universidades, el sector privado y agencias gubernamentales, para desarrollar soluciones contextualizadas a las amenazas de la región.

5.4. Articulación con el sector privado y la sociedad civil

Dado que muchos actores no estatales provienen del mundo corporativo y digital, el Estado debe construir alianzas estratégicas con actores privados, especialmente en sectores sensibles, como telecomunicaciones, servicios financieros, *big tech*, transporte logístico, vigilancia privada y medios digitales. Esta articulación no debe limitarse a la firma de convenios, sino a la construcción de esquemas de gobernanza colaborativa, ciberresiliencia compartida y responsabilidad colectiva frente a amenazas híbridas.

Asimismo, la sociedad civil —las ONG, la academia, las comunidades técnicas y los medios independientes— debe ser incorporada en el monitoreo, la evaluación y la

auditoría de estas políticas, para garantizar que los derechos digitales, la privacidad y la transparencia no sean sacrificados en nombre de la seguridad.

5.5. Cultura estratégica y pedagogía del riesgo

Finalmente, ningún diseño institucional será suficiente si no se produce una transformación cultural. América Latina requiere construir una cultura estratégica del riesgo, que incluya:

- Concientización ciudadana sobre amenazas digitales, desinformación, fraude, violencia cibernética y espionaje.
- Alfabetización digital crítica desde la educación básica hasta la universitaria.
- Simulacros y planes de continuidad de negocios frente a ataques híbridos.
- Campañas de prevención y pedagogía del autocuidado en entornos digitales.

La construcción de esta cultura no es un lujo, sino una necesidad para reducir la vulnerabilidad estructural de nuestras sociedades y para evitar que el miedo y la desinformación debiliten aún más la legitimidad estatal.

Conclusión

La emergencia de actores no estatales tecnológicamente empoderados y la transformación de los conflictos hacia formas híbridas, automatizadas y multidominio representan un cambio estructural en la lógica de la seguridad internacional. Este fenómeno —acelerado por el acceso masivo a tecnologías de uso dual, la descomposición de las fronteras entre lo legal e ilegal y la fragmentación de los monopolios estatales sobre la coerción y la información— plantea desafíos inéditos para los Estados, en particular, para aquellos con capacidades institucionales limitadas, como muchos de América Latina.

La región se enfrenta a una amenaza estratégica que ya no se limita al crimen organizado tradicional o a la violencia callejera. Se trata ahora de redes transnacionales que combinan sofisticación técnica, poder económico, capital social y acceso a herramientas de manipulación informativa y vigilancia digital. Estos actores operan con agilidad, sin fronteras, sin escrúpulos y, en muchos casos, con la colaboración —por acción u omisión— de segmentos del sector privado, del aparato estatal o de la ciudadanía. La pregunta ya no es si estos actores tienen poder, sino cuánto poder pueden seguir acumulando sin que los Estados pierdan capacidad de regulación, respuesta y legitimidad.

Esta situación es particularmente crítica en América Latina, donde la desigualdad, la fragmentación territorial, la debilidad institucional y las brechas tecnológicas crean un entorno fértil para el crecimiento de estas amenazas. Al mismo tiempo, el desbalance entre las capacidades estatales y las de los actores no estatales —legales o ilegales— se amplía a un ritmo preocupante, lo que genera asimetrías internas

(entre agencias estatales), regionales (entre países) y funcionales (entre Estados y actores extraestatales).

En este contexto, se vuelve urgente superar la visión fragmentaria, reactiva y defensiva que muchas veces caracteriza las políticas públicas de seguridad. América Latina no puede seguir relegando la seguridad al último lugar de la agenda gubernamental, como si se tratara de un problema exclusivamente policial o de control del orden. La seguridad ya no es un asunto sectorial, sino una condición estructural para el ejercicio de la soberanía, la consolidación democrática, la protección de derechos y la viabilidad misma del desarrollo económico y social.

No hay seguridad sin desarrollo, pero tampoco hay desarrollo sin seguridad. En demasiados países de la región, los Gobiernos están concentrados casi exclusivamente en atraer inversiones, generar crecimiento y expandir programas sociales, mientras que la seguridad es tratada como un costo reactivo, externalizado o diferido. Esta visión desequilibra el ecosistema institucional y deja la iniciativa en manos de actores criminales, paramilitares o corporativos informales, que diseñan las reglas del juego *de facto*. El Estado, lejos de ser un *rule-maker*, deviene un *rule-taker*, limitado a gestionar el daño y administrar el descontrol. La ausencia de políticas preventivas, de una cultura estratégica de anticipación y de sistemas de inteligencia proactiva ha colocado a los Estados en una posición subordinada dentro del nuevo tablero geopolítico de la seguridad.

En consecuencia, se impone la necesidad de una reconfiguración profunda de las capacidades estatales, tanto en lo normativo como en lo operativo, lo estratégico y lo simbólico. Esto incluye:

- La transformación del Estado en un actor anticipatorio y no reactivo.
- La generación de capacidades tecnológicas endógenas que reduzcan la dependencia de proveedores externos.
- El fortalecimiento del vínculo entre seguridad, defensa, justicia, relaciones exteriores, ciencia y tecnología, desarrollo y derechos humanos.
- La recuperación del rol rector del Estado frente al poder de actores privados en materia de vigilancia, seguridad digital y control informacional.
- Y, sobre todo, la articulación regional para construir respuestas colectivas ante amenazas que, por definición, exceden las fronteras nacionales.

América Latina no está condenada a ser el eslabón débil de la seguridad global. Tiene capacidades, recursos, talento humano y potencial estratégico. Pero, para aprovecharlos, debe asumir con realismo, coraje y visión de futuro los desafíos de la posmodernidad conflictiva. El tiempo de las advertencias ha terminado. Lo que está en juego no es simplemente la seguridad de los Estados, sino la posibilidad de construir sociedades libres, inclusivas y viables en el siglo XXI.

Referencias

Bayart, J. F. (2000). Africa in the world: A history of extraversion. *African Affairs*, 99(395), 217-267. https://doi.org/10.1093/afraf/99.395.217

Flor-Unda, O., Simbaña, F., Larriva-Novo, X., Acuña, Á., Tipán, R. y Acosta-Vargas, P. (2023). A Comprehensive Analysis of the Worst Cybersecurity Vulnerabilities in Latin America. *Informatics*, 10(3), 71. https://doi.org/10.3390/informatics10030071

FMI y GAFILAT. (2023). *Informe de evaluación mutua de la República de Colombia*. https://biblioteca.gafilat.org/wp-content/uploads/2024/07/IEM-Colombia-4taRonda.pdf

Fukuyama, F. (2004). *State-Building: Governance and world order in the 21st century*. Cornell University Press.

Global Financial Integrity. (2021). *Trade-realted llicit financial flows in 134 Developing Countries 2009-2018*. https://gfintegrity.org/report/trade-related-illicit-financial-flows-in-134-developing-countries-2009-2018/

Hammes, T. X. (2004). *The sling and the stone: On war in the 21st century*. Zenith Press.

International Crisis Group. (2023). *Latin America Wrestles with a New Crime Wave*. wl-latam-spring-2023.pdf

Kaldor, M. (2012). *New and old wars: Organized violence in a global era* (3.ª ed.). Stanford University Press.

Lind, W. S., Nightengale, K., Schmitt, J. F., Sutton, J. W. y Wilson, G. I. (1989). The changing face of war: Into the fourth generation. *Marine Corps Gazette*, 73(10), 22-26.

Organización para la Cooperación y el Desarrollo Económico. (2021). *Latin America and the Caribbean: Latin America and the Caribbean and the OECD*. https://www.oecd.org/latin-america

Organización de los Estados Americanos (OEA). (2022). *Seguridad Multidimensional: Programas, Proyectos e Iniciativas*. CICTE. https://www.oas.org/ext/es/seguridad/prog-cibe

Reed, D. J. (2008). Beyond the war on terror: Into the fifth generation of war and conflict. *Studies in Conflict & Terrorism*, 31(8), 684-722. https://doi.org/10.1080/10576100802206533

Rotberg, R. I. (2003). *State failure and state weakness in a time of terror*. Brookings Institution Press.

United Nations Development Programme. (2022). *Tiempos inciertos, vidas inestables: Configurar nuestro futuro en un mundo en transformación*. https://doi.org/10.18356/9789210016421

United Nations Office on Drugs and Crime. (2012). *Transnational Organized Crime in Central America and the Caribbean: A Threat Assessment*. https://www.unodc.org/documents/data-and-analysis/Studies/TOC_Central_America_and_the_Caribbean_english.pdf

World Economic Forum. (2023). *Global risks report 2023*. https://www.weforum.org/reports/global-risks-report-2023/