Capítulo 9

Operaciones de interferencia en ciberseguridad y ciberdefensa: herramienta estratégica para la supervivencia de los Estados*

DOI: https://doi.org/10.25062/9786289530483.09

Felipe Eduardo Rodríguez Álvarez
Luis Alexander Montero Moncada
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: El presente capítulo tiene como objetivo determinar la importancia y capacidad estratégica para las naciones de las operaciones de interferencia en escenarios como el ciberespacio. Para ello, en primer lugar, se determinan los principales conceptos en las operaciones de interferencia en ciberseguridad y ciberdefensa, desde las relaciones internacionales y la doctrina militar. Enseguida, se describe la forma en que las operaciones de interferencia en ciberseguridad y ciberdefensa favorecen el poder de los Estados, desde las relaciones internacionales y las Ciencias Militares. Luego, se analizan operaciones de interferencia en ciberseguridad y ciberdefensa internacional desarrolladas con éxito en naciones como Israel, y, finalmente, se describen las posibilidades de éxito de las operaciones de interferencia en ciberseguridad y ciberdefensa por parte de Colombia, mediante los factores de inestabilidad.

Palabras clave: amenazas; ciberseguridad; factores de inestabilidad; inteligencia; operaciones de interferencia.

* Este capítulo presenta los resultados del proyecto de investigación "Poder y Estrategia. Fundamentos para la supervivencia del Estado" del grupo de investigación "Centro de Gravedad" de la Escuela Superior de Guerra "General Rafael Reyes Prieto", categorizado en A por Minciencias y con código de registro COL0104976. Los puntos de vista pertenecen a los autores y no reflejan necesariamente los de las instituciones participantes.

Felipe Eduardo Rodríguez Álvarez
Teniente Coronel del Ejército Nacional de Colombia. Magíster en Inteligencia Estratégica, Escuela de Inteligencia y Contrainteligencia "Brigadier General Ricardo Charry Solano"; especialista en Seguridad Integral y Análisis de Riesgos, Escuela de Inteligencia y Contrainteligencia-ESICI, y profesional en Ciencias Militares, Escuela Militar de Cadetes "General José María Córdova".

Luis Alexander Montero Moncada
Candidato a doctor en Estudios Políticos, Universidad Externado de Colombia, y en Estudios Políticos y Relaciones Internacionales, Universidad Nacional de Colombia; magíster (honoris causa) en Inteligencia Estratégica, Escuela de Inteligencia del Ejército "Brigadier General Ricardo Charry Solano", y en Análisis de Problemas Políticos, Económicos e Internacionales Contemporáneos, Instituto de Estudios Políticos de París Sciences-PO, Universidad Externado de Colombia y Ministerio de Relaciones Exteriores de Colombia; politólogo con énfasis en Relaciones Internacionales, Universidad Nacional de Colombia.
Orcid: https://orcid.org/0000-0003-3420-0863 - Contacto: luis.montero@esdeg.edu.co

Citación APA: Rodríguez Alvarez, F. E. & Montero Moncada, L. A. (2022). Operaciones de interferencia en ciberseguridad y ciberdefensa: herramienta estratégica para la supervivencia de los Estados. En A. Montero Moncada (Ed), *Poder y estrategia. Elementos para la supervivencia del Estado* (pp. 277-301). Sello Editorial ESDEG. https://doi.org/10.25062/9786289530483.09

PODER Y ESTRATEGIA.
ELEMENTOS PARA LA SUPERVIVENCIA DEL ESTADO
ISBN impreso: 978-958-53778-9-9
ISBN digital: 978-628-95304-8-3
DOI: https://doi.org/10.25062/9786289530483

Colección Seguridad y Defensa
Sello Editorial ESDEG
Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia
2022

Introducción

La supervivencia es una de las necesidades prioritarias que tienen las naciones a nivel mundial (Knorr, 1981) y, por lo tanto, debe enfocarse en utilizar estrategias, tareas y capacidades óptimas para eliminar, bloquear y neutralizar cualquier tipo de riesgo nacional. No obstante, en el escenario actual, donde nacen nuevos estilos de guerra, los altos mandos nacionales deben establecer actividades y operaciones en pro de la seguridad y defensa nacional. Para ser considerados territorios soberanos, con límites y representación política internacional, los Estados deben ajustarse a la carrera cosmopolita por el poder, siendo este factor el que incita la exploración de herramientas de contención, reacción y protección de acuerdo a sus intereses.

Para que la supervivencia consiga un nivel de protección y mantenimiento constante, es necesario contar con las capacidades humanas, técnicas y científicas que concurren hoy en día, beneficiando las actividades del poder de los Estados y su constante evolución dentro de las exigencias del orden internacional (Noya, 2005). El desarrollo de la tecnología, la evolución de las ideas y la presión constante por sobrevivir han obligado a las sociedades a constituir destrezas que permitan la no materialización de riesgos que atenten contra la institucionalidad e integridad estatal.

Las estrategias y capacidades con mayor intervención y eficacia para sostener la constitucionalidad e integridad de las naciones son el tridente estratégico, la base operativa para la estabilidad nacional (Algaba et al., 2005). Esta consiste en la unión de capacidades ejecutantes de las FF. EE., soportados por la recolección de datos de la inteligencia y protegidos por las barreras de la ciberdefensa, enfocados en minimizar los riesgos y la no materialización de amenazas en ambientes tanto bélicos como de diplomacia (Gruer, 2013). Al llevar a cabo actos de

defensa nacional, los intereses nacionales son protegidos por la participación activa de las instituciones estatales con responsabilidades estratégicas, pues bajo su dominio se encuentra el aseguramiento a la soberanía, la independencia nacional, la unidad, la integridad territorial y la constitución de la democracia (Velarde, 2020).

La funcionalidad y efectividad de las decisiones de los altos mandos, incluso con un alto impacto estratégico, en ocasiones pasa inadvertida por falta de conocimiento respecto de las ventajas, destrezas y proezas que acatan las actividades de interferencia desarrolladas por componentes como el tridente estratégico de las naciones (González, 2015). Dadas estas circunstancias, resulta pertinente enmarcar una actividad investigativa que responda de forma académica, científica y comprobable a la pregunta: ¿Cuál es el aporte de las operaciones de interferencia en ciberseguridad y ciberdefensa como herramienta estratégica para la supervivencia de los Estados?

En tal sentido, en el presente artículo se determinan, en primer lugar, los principales conceptos en las operaciones de interferencia en ciberseguridad y ciberdefensa, desde las relaciones internacionales y la doctrina militar. Enseguida, se describe la forma en que las operaciones de interferencia en ciberseguridad y ciberdefensa favorecen el poder de los Estados, desde las relaciones internacionales y las Ciencias Militares (CC. MM.). Luego, se analizan operaciones de interferencia en ciberseguridad y ciberdefensa internacional desarrolladas con éxito en naciones como Israel, y, finalmente, se describen las posibilidades de éxito de las operaciones de interferencia en ciberseguridad y ciberdefensa por parte de Colombia, mediante los factores de inestabilidad.

Marco conceptual

Seguridad y defensa nacional

Para precisar la definición de seguridad y defensa nacional como un todo, es necesario examinar sus componentes de forma individual. Seguridad nacional es aquel requisito esencial de todos los ámbitos de la vida pública, así como las necesidades básicas de todos los sistemas naturales y sociales (Almazán, (2015). Como parte constituyente del mandato del Estado democrático, es la base para la acción y la planificación de las políticas públicas, donde se enfrentan enormes desafíos no solo en la defensa contra peligros potenciales extremos como el terrorismo o las catástrofes, sino con diferentes fenómenos que atentan contra la

integridad y constitución de los Estados. Aunque muchas áreas de investigación se ocupan de la seguridad y es parte de varios discursos, conceptualmente sigue siendo un concepto poco claro que está sujeto a cambios permanentes.

Defensa nacional, por otra parte, son aquellas acciones estatales desarrolladas para proteger intereses de orden estratégico, actuando principalmente de forma preventiva ante el surgimiento de enfrentamientos paralizantes para la constante evolución y desarrollo de las naciones (Dussan, 2005). Por lo general, cuando ocurre un agrietamiento interno, este componente invita a la intervención extranjera que amenaza de forma directa la defensa de los territorios.

Ante ello, la unión de los conceptos de seguridad y defensa nacional representa un reto para los entes académicos y científicos, ya que los departamentos de Defensa y Seguridad del mundo aun sostienen discusiones operativas y de aplicación para tal concepto. Para aclarar, no obstante, las siguientes líneas, diremos que la seguridad y la defensa son dos elementos que exaltan la propiedad de protección, donde no se materializan riesgos, perjuicios ni peligros y fabrican cierto nivel de confianza a todos los sujetos que integran los Estados, pues es claro que conviven una serie de elementos tanto oriundos, como terrestres que deben ser defendidos y salvaguardados del alcance de personas que no les corresponde dirigirlos ni aprovecharlos. Sin embargo, esta diligencia de seguridad no se forma simplemente con un plan, pues debe estar forjada y plasmada por alguna ley, orden, tarea o ruta política para enfrentar cualquier tipo de amenaza.

Operaciones encubiertas

Ante las circunstancias que prosperan en los términos de seguridad y defensa, existen herramientas operacionales que intervienen en la recolección de datos y que, en su mayoría, garantizan un adecuado procesamiento para convertirlos en información de alto valor para la protección de los Estados. Entre estas acciones, las operaciones encubiertas son una de las capacidades que aun siendo de alto riesgo, generan resultados de alto impacto para la toma de decisiones (Almaraz, 2016:

> Una operación encubierta es aquella acción de investigación que ejecuta la autoridad con el propósito de hacer creer a los delincuentes que se está actuando a la par de ellos, es decir, que también los que actúan en la operación encubierta, que son los agentes de policía infiltrados, lo hacen ilícitamente, sin pensar los miembros de la organización delictiva, que es una farsa, un engaño, con el objeto de hacer creer que igual que ellos se está actuando impunemente. (p. 149)

Generalmente, las operaciones encubiertas logran desarrollarse cuando los decisores políticos solicitan datos que no consiguen por medio de la búsqueda de diferentes fuentes como las abiertas (Open Source INTelligence, OSINT); en gran medida es una herramienta de bastante aplicación a lo largo y ancho de las naciones.

Inteligencia estratégica

Es un proceso de recopilación, procesamiento, análisis y difusión de inteligencia crucial en la formulación de políticas (Liebowitz, 2006). Puede ser vista en perspectiva y es una herramienta para que una organización pueda proyectar su funcionamiento y su entorno, entre otros. Esto se logra mediante el diseño de estrategias adecuadas, alineadas con la visión y misión de la organización. La inteligencia estratégica es una combinación de diferentes tipos de inteligencia, como inteligencia comercial y competitiva inteligencia que crea una sinergia en la inteligencia y el conocimiento de una organización, facilitando la adquisición de información valiosa en la decisión organizativa.

Por otro lado, la inteligencia estratégica es información que se necesita para formular políticas y planes militares en los niveles de política nacional e internacional (Sainz de la Peña, 2012). Gracias a ello, la inteligencia táctica está destinada principalmente a responder a las necesidades de los comandantes de campo militares para que puedan planificar y, si es necesario, realizar operaciones de combate. Esencialmente, la inteligencia táctica y la inteligencia estratégica solo difieren en el alcance, el punto de vista y el nivel de empleo.

Inteligencia militar

La recolección de información debe desarrollarse bajo los conceptos actualmente avalados, entre ellos, la inteligencia (Jasso, 2017). Esta incluye las divisiones y clasificaciones acatadas por los organismos internacionales, generando protagonismo a los actos establecidos por las instituciones militares. Por ello, la inteligencia militar es expuesta como aquella capacidad que incluye todas las disciplinas dedicadas a la recopilación, análisis y difusión de información para unidades militares y tomadores de decisión (Mendoza, 2020).

Según el Manual Fundamental del Ejército, MFE, 2-0 (2017), la inteligencia militar se divide en Contrainteligencia (CI); Inteligencia Humana (HUMINT, por su sigla en inglés); Inteligencia Geoespacial (GEOINT, por su sigla en inglés); Inteligencia de Señales (SIGINT, por su sigla en inglés); Inteligencia Técnica

(TECHINT, por su sigla en inglés); Ciberinteligencia (CIBINT); Guerra Electrónica (EW, por su sigla en inglés); Inteligencia de Medidas y Huellas Distintivas (MASINT, por su sigla en inglés), e Inteligencia de Fuentes Abiertas (OSINT, por su sigla en inglés). Las actividades de inteligencia se llevan a cabo en todos los niveles, táctico, operativo y estratégico, ya sea en tiempos de paz o de guerra.

Contextualización de las operaciones de interferencia en escenarios cibernéticos

Conceptos de operaciones de interferencia en ciberseguridad y ciberdefensa

En el escenario que actualmente viven las naciones, es posible identificar la necesidad de defensa y seguridad de las mismas. Ningún gobernante puede definir su periodo presidencial sin exponer, acatar y delimitar las formas, estrategias y actos que permitirán la armonía estatal a la que se confiere, desde el inicio, su labor como presidente. Esta labor es soportada con asesorías y acompañamientos de las estructuras e instituciones fundamentales para las naciones, reconocidas como inherentes de la estructura política de las mismas (Sanahuja & Verdes-Montenegro, 2014).

Entre ellas es posible reconocer que muchos de sus actos son avalados por estrategias de orden militar, político y diplomático, siendo la diplomática una de las vías de mayor ejecución y manifestación en el orden internacional (Spielman, 2011). Entre las actividades diplomáticas están las operaciones de interferencia que son avaladas y permitidas mientras se coincida con la necesidad de proteger y salvaguardar los intereses nacionales (Saddiki, 2009). Estas operaciones son una de las herramientas de la política exterior de las naciones que utilizan los formuladores de políticas para promover los intereses nacionales (Cull, 2009) y se utiliza en esfuerzos internacionales selectos, pues abarca una amplia gama de actividades fuera de las operaciones de recopilación de inteligencia tradicional. Generalmente, la acción de interferencia puede proporcionar resultados e información que de otro modo no estaría disponible. Aunado a ello, las actividades que integran las operaciones de interferencia influyen en las condiciones políticas, económicas o militares en el extranjero, donde se pretende que la intención del perpetrador o autor de estas no sea evidente o reconocido públicamente (Berenstein, 2004).

Para enfatizar en los conceptos operacionales de interferencias en ciberseguridad y ciberdefensa, es necesario ilustrar por medio de ejemplos literarios su actuación. Por ello, al suponer dos actores A y B, se reconoce que son dos Estados, cada uno con intereses y objetivos estratégicos que cumplir; no obstante, el país A encuentra llamativo algún bien, servicio o material útil para la supervivencia en el país B, y comienza a actuar dentro o fuera de la legalidad para conseguirlo. Si los actos de A son explícitos, en organizaciones y tribunales internacionales se podría intervenir para finalizar con su cometido. Pero, cuando estos no logran sustentarse por la falta de pruebas que concurran en sus actos, es posible considerar este tipo de actos como interferencias. Las acciones de interferencia adecuadas se llevan a cabo porque los legisladores, no las agencias de inteligencia, creen que los medios secretos son la mejor manera de lograr un fin deseado o un objetivo político específico (Luna, 2014).

Ante el ejemplo gráfico previamente descrito, autores como Fernández et al., (2013) expresan que la interferencia es aplicada a aquellas actividades que limitan la expansión, proyección o supervivencia de algún Estado. Típicos eventos de la misma se evidencian cuando Ávila et al., (2013) exponen los intereses políticos de naciones como la venezolana, ya que la protección o apoyo a las guerrillas colombianas generan consecuencias de gran envergadura para la seguridad y defensa de Colombia. Aquí, la interferencia dirigida por mandatarios como Hugo Chávez y Nicolás Maduro interfieren de forma negativa para Colombia, pero, de forma positiva para los intereses de los mandatarios venezolanos. Ante ello, cuando una acción, suceso o actividad subestima las barreras de protección e integridad de las naciones, resulta necesario y de urgente uso la estrategia promovida por la interferencia, pues su ejecución mantiene el nivel de secreto y exclusividad cuando suele manejarse en niveles de toma de decisión como el estratégico.

Ajuste pragmático desde las Ciencias Militares

Si se conciben las operaciones de interferencia como una de las acciones promovidas por los ámbitos militares, es posible reflejar este tipo de acciones en sucesos como los liderados por naciones como EE. UU. (Roca, 2013). Generalmente, la acción de interferencia desarrollada por esta nación tiene como objetivo influir en las condiciones de seguridad que podría conducir a un compromiso militar considerable o extendido (Sala, 2018). A diferencia de la recopilación de datos de la inteligencia tradicional, las operaciones de interferencia no son pasivas. Estas

tiene un impacto público visible destinado a influir en un cambio en el entorno militar, económico o político en el extranjero que, de lo contrario, podría resultar contraproducente si se diera a conocer el papel del autor generador de las mismas (García, 2012).

Para generar entonces posibles actos de interferencia liderados por las estructuras militares, estas podrían ir de la mano con actos psicológicos y de inclusión para la ciudadanía; por ejemplo, los actos de propaganda son uno de los medios por los cuales personal militar especializado en inteligencia hace explícito uso de ellas (López, 2015). Las agencias de inteligencia difunden de forma encubierta información específica para promover los objetivos de la política exterior del Estado (Caballero, 2004). Por otro lado, estas acciones son paralelas a la acción política y económica de interés, ya que las agencias de inteligencia influyen también de forma encubierta en el funcionamiento político o económico de una nación foránea.

Por otro lado, las operaciones de interferencia suelen encontrarse en las Ciencias Militares (CC. MM.) en las acciones y operaciones militares a cubierta; en ellas, las agencias de inteligencia entrenan y equipan de manera encubierta al personal para atacar a un adversario o para realizar operaciones de recolección de información (Monsálvez, 2013). Estas operaciones, normalmente no implican el uso de personal militar uniformado como combatientes, ya que permiten la diversidad de papeles que reubiquen la verdadera línea cotidiana del agente por utilizar. No obstante, si esta línea táctica de interferencia se cruza con tiempos de guerra o conflicto armado, es posible que las naciones líderes de las mismas necesiten hacer uso de la fuerza letal encubierta contra enemigos (McSherry, 2009).

Ante ello, entre los actos de materialización a que se recurre en las operaciones militares y su campo de aplicación para las tareas de interferencia, es necesario considerar la combinación de dos componentes del tridente estratégico: FF. EE. e inteligencia (Ferreira, 2006). Si bien, al suponer que estos actos son capacidades propias para expandir las actividades de interferencia en las naciones, se recurre entonces al factor humano militar que sostiene el mejor entrenamiento y capacitación ante el desarrollo de operaciones de un alto nivel e impacto. Ejemplos como el de Israel, que era constantemente amenazado por sus vecinos, ya fuera directamente por la guerra o indirectamente por el terrorismo, se mantuvo, no obstante, algo alejado de la Guerra Fría, dando a sus operaciones de interferencia un valor distintivo y convirtiendo al país en un líder mundial en las capacidades de inteligencia (Ferreira, 2006).

Esta nación tiene muchas lecciones para los servicios de inteligencia de Occidente que se están adaptando lentamente a este entorno político tan diferente. Estas, pueden reconocerse por medio de tres frentes principales: 1. Contraterrorismo, 2. Contra la proliferación nuclear o adquisición de tecnología y 3. Ayuda humanitaria (Sánchez, 2001).

En el primer bloque, los israelíes reaccionaron rápida y duramente contra el terrorismo internacional, utilizando equipos del Mossad que operaban de forma encubierta en muchos países extranjeros (San Felipe Donlo, 2013). Muestra de ello fue la acción de Shin Beth, quien entrenó guardias ocultos armados con pistolas de baja velocidad que se colocaron en aviones israelíes listos para participar en batallas aéreas con cualquier secuestrador. A su vez, agentes del Mossad y Shin Beth se infiltraron en los campamentos de Cisjordania para recibir advertencias de ataques terroristas. También operaron en Jordania, transmitiendo información al rey Husein; algunos de estos agentes eran espías, otros actuaban en un papel diplomático encubierto, organizando reuniones secretas entre los líderes israelíes y el rey Husein (Mesa del Monte, 2007).

En el segundo bloque, en materia de servicios secretos involucrados en tratar de robar secretos industriales y técnicos, los israelíes tienen un historial solo superado por la KGB (Bar-Zohat et al., 2013). En la década de 1960, se estableció una organización especial y altamente secreta llamada Lekem, adjunta al Mossad. La función de Lekem es la recopilación de inteligencia científica y técnica. Sus agentes viajan de forma encubierta como hombres de negocios y científicos o son adscritos al personal de las embajadas israelíes en todo el mundo (Gruer, 2013). Tradicionalmente, Lekem se ha centrado en dos áreas: tecnología militar y tecnología nuclear, con cierto éxito notable en ambas áreas. El Mossad también ha trabajado para eludir los embargos de armas impuestos a Israel (Róbalo, 2016).

Ante estas circunstancias, el escenario israelí es definido como un Estado acosado por enemigos (Buzan, 1991). Aquí, la búsqueda permanente de seguridad, lleva a Israel a tomar acciones que amplían su espectro de amenaza antes que mejorarlo, careciendo entonces de la influencia política o económica de naciones más grandes y poderosas. Ante ello, los israelíes han utilizado operaciones encubiertas para lograr objetivos de política exterior, como ayudar a prevenir la proliferación nuclear, al mismo tiempo que ayudan al desarrollo de sus propias armas (Abad, 2014). Estos ejemplos hacen parte de las operaciones de interferencia de naciones con una alta participación de personal de capacidades como

la inteligencia, la cual suele aliarse con las habilidades humanas que concurren en las estrategias de FF. EE., que pueden generar algunos requisitos de inteligencia, en sus guías de estudio de área, antes de la implementación (Rodríguez & Jordán, 2015).

En otros casos, las agencias nacionales de inteligencia pueden mantener al día a las unidades de operaciones especiales haciendo lo que siempre han hecho y en cómo han llevado a cabo las operaciones en el pasado (Gómez, 2004). Para las unidades de FF. EE. desplegadas en actos de interferencia, la protección de la fuerza es un factor extremadamente importante en la seguridad general de la misión (Jordán, 2016). Aquí, las redes de inteligencia locales deben organizarse y dotarse de recursos, donde pueden adaptarse a la misión y al área operativa. Por ello, las FF. EE. tienen personal excepcionalmente capacitado, ya que logran detectar, evaluar, desarrollar y reclutar fuentes de bajo nivel para los requisitos de protección de las naciones (Rodríguez, 2016). Estas operaciones son extremadamente importantes en las áreas operativas de protección de la fuerza y alerta temprana.

Percepción desde las relaciones internacionales

Al entender su aplicación militar por medio de la capacidad humana de las FF. EE. y las tácticas de recolección de información de la inteligencia, las operaciones de interferencia se exponen al señalamiento y posible persecución de otras naciones en el orden internacional. Dadas estas circunstancias, es necesario orientar estas intervenciones bajo la teorías y consideraciones de las RR. II. (Barba, 2015). Al menos en los últimos veinte años las RR. II. han permitido que se incluyan las actividades que suscitan de los roles diplomáticos y sus funciones como intermediarios internacionales (Azpíroz, 2012). Ante ello, diplomáticos de muchos países están involucrados en tareas tales como la búsqueda de la solución a los conflictos regionales, apoyo en asistencia humanitaria, mediaciones en los problemas ambientales globales y en la cooperación económica internacional, teniendo claro que estas acciones son una puerta de entrada de *soft power* en las intenciones de interferencia internacional.

Aquí, los diplomáticos y sus actividades son la figura teóricamente avalada que acepta involucrar a los Estados en mucha mayor medida y con mucha mayor relevancia que durante las cuatro décadas anteriores. En el pasado, la diplomacia era una profesión prestigiosa, pero discreta, no siempre llevada a cabo con prudencia fuera de los ojos del público (Riordan, 2005). Hoy en día, los

propios diplomáticos se están convirtiendo en el blanco de los medios y del público internacional. Cabe resaltar que la diplomacia, en el uso de negociaciones para promover los intereses internacionales de un Estado, sigue desempeñando un papel importante en el ajuste de los intereses estatales y las sociedades a los desafíos contemporáneos.

Generalmente, los principios diplomáticos se centran en el nivel operativo, es decir, el nivel de las comunidades de política exterior donde los profesionales planifican, diseñan y conducen la diplomacia para lograr objetivos en el interés estratégico nacional (Muñoz, 2015). En asuntos militares, el nivel operativo es crucial en la ejecución de tareas militares, vinculando el empleo táctico de fuerzas con objetivos estratégicos nacionales y militares. Aquí, la diplomacia, como teoría de las RR. II., fusiona objetivos estratégicos con medios y recursos diplomáticos (León Gross, 2019). La diplomacia a nivel operativo puede describirse como actividades deliberadas que vinculan el empleo de recursos diplomáticos con los objetivos de la política exterior nacional. Este nivel, justo por debajo del de toma de decisiones estratégicas y estrechamente relacionado con las tácticas y técnicas de negociación, es lo suficientemente distinto como para que la introducción de algunos principios coherentes pueda ser útil para los profesionales diplomáticos operativos.

Favorecimiento operativo y estratégico de las operaciones de interferencia hacia el poder de los Estados

Entre los intereses que existen en el orden internacional, hay una percepción muy considerable sobre la insatisfacción de los gobernantes respecto del concepto de poder (Cancelado, 2010). Esta situación surge porque las nociones tradicionales de Estado y de poder se encuentran fuera y distantes de las condiciones políticas actuales (Ghotme, 2011). Este poder, que hace parte de los intereses estratégicos de los territorios, es considerado como una prioridad, y, al ser una prioridad, encaja de forma directa en la necesidad de protegerlo, fomentarlo, reforzarlo o administrarlo.

El manejo o exposición de los niveles de poder estatal en el mundo hacen parte de la adaptación de tareas, políticas y acciones del nivel estratégico nacional, y este, al tener la calificación de prioritaria, puede fomentarse por

medio de herramientas como la diplomacia, la intervención militar y el dominio de las RR. II., entre otros (Fradkin, 2011). El orden militar, una herramienta común y de alto uso, es aquella condición inherente que activa acciones de interferencia, entendiendo que tanto las acciones bélicas como la búsqueda de la información hacen parte del rol de protección de los altos gobernantes (Porras, 2004).

Con miras a direccionar las actividades de interferencia como una herramienta de orden estratégico, es necesario encasillar un concepto básico de poder. En efecto, poder se refiere a la capacidad que tiene un actor de controlar a otro para hacer lo que ese otro no haría de otra manera (Ávila-Fuenmayor, 2006). Al mostrar favoritismo conceptual, la disciplina no solo pasa por alto las diferentes formas de poder en la política internacional, sino que tampoco logra desarrollar una comprensión sofisticada de cómo se producen los resultados globales y cómo los actores están capacitados y limitados de manera diferencial para determinar su destino.

Cuando un Estado presenta entonces estrategias que promuevan, protejan y establezcan su poder, la aplicación de medidas políticas, diplomáticas o militares son avaladas y aprobadas por cualquier dominio internacional (Aguiló, 2009). En efecto, es muy común presentar el uso de actividades militares ante escenarios que promuevan la protección y la defensa de un territorio, sobre todo cuando esa nación mantiene y desarrolla aspectos como la inteligencia.

Ante estas circunstancias, las nociones de seguridad y estabilidad son fundamentales para la sociedad contemporánea (Dussan, 2005). La seguridad y defensa son un pilar importante de un sistema democrático ante las consideraciones expuestas por el orden internacional. Por ello, la capacidad o incapacidad de brindar seguridad cuestiona la forma en que los Estados generan sus actos de defensa, entendiendo que, cuanta menos seguridad, menor es su poder ante las amenazas y riesgos que suscitan en la era contemporánea.

La inteligencia, asociada con actos como la interferencia, es vista como aquella estrategia que proporciona avisos, información y datos de un alto nivel estratégico para las decisiones de los Estados (San Julián, 2017). Por ejemplo, cuando en un sector mundial existen tensiones por conflictos, economía, diferencias ideológicas, entre otras, es claro que sus diferencias materializan una amenaza inminente. Esta amenaza logra ser identificada, neutralizada y controlada cuando se acatan las capacidades generadas por subsistemas como la inteligencia, que, en efecto, es líder de las actuaciones de interferencia.

Esta interferencia es una operación de inteligencia mediante la cual los Gobiernos, grupos militares, empresas y otras organizaciones recopilan y evalúan sistemáticamente información con el fin de descubrir las capacidades e intenciones de sus rivales (Cofré, 2012). Con dicha información, una organización puede protegerse a sí misma de sus adversarios y aprovechar sus debilidades. En un futuro próximo las agencias de inteligencia y los Gobiernos dependerán cada vez más de esos mecanismos de alerta que puedan responder con prontitud a una tarea aún más y complicada, la prevención de la seguridad (Keejan, 2012).

Éxito operacional de las acciones de interferencia: caso Israel

Para autores como Thomas y Gambolini (2001), el Estado de Israel se estableció solo hasta 1948. No obstante, en sus años de existencia ha tenido una comunidad de inteligencia que, a nivel mundial, es reconocida como una de las más profesionales y efectivas. El Mossad se ha convertido en la agencia líder en el conflicto con los estados árabes. Su misión, no solo incluye la de determinar los planes y las fortalezas de las fuerzas militares árabes que se oponen a Israel, sino también el trabajo de combatir el terrorismo de objetivos israelíes y judíos, recopilar datos técnicos sensibles y realizar operaciones de enlace político y de interferencia (Donlo, 2013).

Esta se compone de cuatro componentes separados: 1. El Mossad es responsable de la recopilación y las operaciones de inteligencia en países extranjeros; 2. La Agencia de Seguridad de Israel controla la seguridad interna y la inteligencia dentro de los territorios ocupados; 3. La Inteligencia Militar es responsable de recopilar inteligencia militar, geográfica y económica, particularmente en el mundo árabe y a lo largo de las fronteras de Israel, y 4. El Centro de Investigaciones Políticas del Ministerio de Relaciones Exteriores prepara el análisis para los encargados de la formulación de políticas gubernamentales sobre la base de documentos analíticos y de inteligencia (Bedman, 2012).

Ante esta conformación, la historia ha datado numerosas ocasiones en que Israel ha generado misiones de interferencia exitosas. Entre estas, se cuenta la operación Olympic Games (2008-2010), representativa y mundialmente reconocida por la interferencia desarrollada en la instalación nuclear de Natanz (Irán), donde se destruyeron sus centrifugadoras por medio del gusano Stuxnet en operación conjunta con naciones como EE. UU., Reino Unido, Países Bajos y Francia (Silva, 2018).

Israel y EE. UU. no generaron sorpresa alguna por la larga historia de estrecha cooperación de inteligencia, ya que concurren en varios momentos históricos como aliados de orden estratégico. Aparte de la provisión regular de inteligencia estratégica y política útil, las guerras de Israel contra los ejércitos árabes entrenados y armados por los soviéticos proporcionaron información invaluable sobre la doctrina militar y los sistemas de armas soviéticos (Pastor, 2017). A finales de la década de 1970 y principios de la de 1980, Israel hizo una contribución única y particularmente valiosa al arrojar nueva luz sobre los misiles balísticos intercontinentales equipados con armas nucleares de Moscú que amenazan a EE. UU.

Esta operación tuvo información recibida de la inteligencia israelita, en que se estableció que Irán se consolidaba como una amenaza de orden nuclear (Anabalón & Donders, 2014). En efecto, se activó entonces la creación de un arma de protección conocida como Stuxnet, un gusano informático de 500 kilobytes que se infiltraba en numerosos sistemas informáticos. Este virus operó en tres pasos: 1. Analizó y apuntó a redes y sistemas informáticos de Windows. 2. Habiéndose infiltrado en estas máquinas, el gusano comenzó a replicarse continuamente, lo que 3. Permitió la intervención en el *software* Siemens Step basado en Windows, entendiendo que este *software* prevalecía y, sigue prevaleciendo, en las redes informáticas industriales, como las instalaciones de enriquecimiento nuclear (Medero, 2012).

Al comprometer al *software* Step, el gusano obtuvo acceso a los controladores lógicos del programa industrial, dando paso al acceso de información respecto de datos industriales cruciales, y les dio la capacidad de operar varias máquinas en los sitios industriales individuales (Fernández, 2018). La efectividad del gusano permitió que más de quince instalaciones iraníes fueran atacadas e infiltradas, y se cree que este ataque fue iniciado por la unidad USB de un trabajador al azar, teniendo instalaciones industriales afectadas como la instalación nuclear de Natanz (Uzal, 2012).

El primer indicio de que existía un problema en el sistema informático de la instalación nuclear fue detectado en 2010. Los inspectores de la agencia internacional de energía atómica visitaron la instalación de Natanz y observaron que una extraña cantidad de centrifugadoras de enriquecimiento de uranio se estaba rompiendo y que la causa de estos fallos se desconocía en ese momento. Más tarde, técnicos de Irán contrataron especialistas en seguridad informática en Bielorrusia para examinar sus sistemas informáticos, descubriendo varios

archivos maliciosos en los sistemas informáticos iraníes (Bejarano, 2012). Posteriormente, se supo que estos archivos maliciosos eran el gusano Stuxnet (García, 2017). Aunque Irán no ha publicado detalles específicos sobre los efectos del ataque, se estima que el gusano Stuxnet destruyó 984 centrifugadoras de enriquecimiento de uranio, disminuyendo en un 30 % la eficiencia del enriquecimiento nuclear (Sáenz, 2020).

Los medios de comunicación, espacios de discusión, intervención de expertos, entre otros, han sido analistas y enfáticos en comprender quién diseñó el gusano Stuxnet y quién fue el responsable de usarlo para atacar esencialmente la instalación nuclear de Irán. Este gusano fue diseñado como un arma cibernética para atacar el desarrollo del programa de desarrollo nuclear de Irán (Illaro, 2014). Los diseñadores del gusano aún se desconocen; muchos expertos sugieren que el ataque del gusano Stuxnet a las instalaciones nucleares iraníes fue una operación conjunta entre EE. UU. e Israel. A pesar de esta especulación, todavía no hay evidencia concreta de quién diseñó el arma cibernética original (Arciniegas, 2018).

Al hacer una evaluación de la efectividad ocasionada por intervenciones como la aplicada con el gusano Stuxnet, es claro que la intención inicial de Israel correspondía a disuadir, neutralizar y controlar el desarrollo progresivo de las armas nucleares. Aun así, señalados o no de ser los responsables de esta actividad, su interferencia generó reacciones a favor de la seguridad del Estado. En este escenario, es necesario considerar el papel esencial y fundamental que juega la comunidad de inteligencia de Israel en la protección del Estado, precisamente cuando se trata de desarrollar sus capacidades en un sistema internacional computarizado, globalizado, turbulento y caótico (Lazar & Costescu, 2018).

Esta nación está librando una guerra por la existencia del país como nación, situación diferenciadora ante otras agencias de inteligencia (Sohr, 2019). Sus dominios, interferencias y representaciones hacen parte de la necesidad internacional de disminuir los actos contra los Estados, situación fundamental ante este tipo de amenazas para la seguridad nacional. Ante ello, varias naciones piden constantemente el acompañamiento de Israel, pues hay varios escenarios donde se están desarrollando no solo las formas clásicas de terrorismo, sino acciones que indiscutiblemente atacan la estabilidad y consolidación territorial. Por ello, es posible considerar en los próximos años la importancia y el éxito operacional israelí en cuestiones de interferencia internacional; su estilo será menos

operativo y estarán más involucrados en otros tipos de espionaje y defensa: menos armas y más ciberdefensa (Reboledo, 2016). La historia de la Comunidad de Inteligencia de Israel es ciertamente inseparable de Israel: siempre estarán en lo que respecta a la seguridad nacional.

Factores de inestabilidad colombianos: oportunidad para las operaciones de interferencia en el escenario cibernético

Al hacer un paralelo que determine la importancia de aplicar las operaciones de interferencia para combatir los factores de inestabilidad de una nación, es necesario destacar la prioridad y viabilidad de estas en este entorno. Este tipo de operaciones se caracteriza además por utilizar teorías y comportamientos de estrategias de armas combinadas, las cuales están dirigidas contra fuerzas enemigas antes de que puedan enfrentarse a las fuerzas amigas en la lucha cuerpo a cuerpo. Estas también contribuyen a establecer las condiciones para la transición a la siguiente fase de una operación, por ejemplo, de la defensa a la ofensa (Jaramillo, 2007).

Ante ello, las operaciones de interferencia no consisten simplemente en atacar a una fuerza enemiga en profundidad (Cordero, 2018). Son la suma de todas las actividades que influyen en las condiciones que las fuerzas enemigas pueden tener comprometidas. Normalmente, este tipo de operaciones incluyen una recopilación de información, adquisición de objetivos, maniobras terrestres y aéreas, actividades ciberelectromagnéticas, y operaciones de información ya sea individualmente o en combinación.

Cuando este tipo de operaciones permite abarcar un contexto amplio y de altos estándares, su utilidad puede parecer efectiva en escenarios donde intervienen los factores de inestabilidad nacional (Spielman, 2007). Estos son factores que pueden cambiar durante un periodo; por ejemplo, las condiciones climáticas, la cantidad de esfuerzo que un individuo aplica a una tarea o el azar, entre otros. En el ámbito nacional, estos factores generalmente aplican a las condiciones bélicas, de riesgo y de amenaza previamente determinadas por los agentes o analistas de seguridad nacional (Francisco, 2003).

Ante ello, las operaciones de interferencia efectivamente logran acaparar una estrategia de aplicación que elimine, neutralice o controle la diseminación de los factores de riesgo. Cuando un factor de riesgo ataca los estándares de

estabilidad de los Estados, las actividades de interferencia tienen el propósito de evitar que las fuerzas o capacidades enemigas logren utilizar sus estrategias bélicas de manera eficaz (Gómez, 2006). Estas podrían tener como objetivo interrumpir el movimiento de reservas operativas o evitar que el enemigo utilice armamento con un largo radio de mortalidad. Por otro lado, estas operaciones también podrían enfocarse en interferir con el proceso de reclutamiento, capacitación o manipulación de los actores enemigos, eliminando de forma directa los actores subyacentes que permiten aumentar la capacidad y recurso humano de la fuerza opositora.

Durante las operaciones de interferencia, sus efectos suelen ser más influyentes cuando se dirigen en contra de la capacidad de un enemigo para comandar, agrupar, maniobrar, suministrar y reforzar los dispositivos convencionales disponibles (Matey, 2017). No obstante, si se dirige este tipo de operaciones ante un enemigo que emplea una estructura de fuerza encubierta, una red logística simple y unas tácticas poco convencionales, suele tener un grado de dificultad mayor. Sin embargo, con inteligencia precisa oportuna y persistente, las operaciones de interferencia pueden interrumpir considerablemente la estabilidad y operatividad del enemigo.

Aquí, los altos mandos pueden utilizar cualquier número de tareas durante la ejecución de operaciones de interferencia ante los factores de inestabilidad para desviar, interrumpir, retrasar y destruir las fuerzas enemigas. Estas acciones no son mutuamente excluyentes, ya que las acciones están asociadas con un efecto que puede apoyar a los otros.

Cualquier factor de inestabilidad, naciente de variedad de campos, puede apoyar la interrupción del comportamiento enemigo, entendiendo el enemigo como ese actor que busca intervenir en los actos de seguridad y defensa de los Estados (Almaráz, 2016). Esto puede materializarse en el empleo de fuerzas, capacidades o sistemas que alteran el ritmo operativo, el flujo de información o la interacción de las fuerzas enemigas y sus sistemas de apoyo. Por ejemplo, en lugar de un esfuerzo enemigo cohesivo, la interrupción puede producir confusión, miedo y resistencia fragmentada. Por lo tanto, interrumpir al enemigo permite tomar, retener y explotar la iniciativa y mantener la libertad de acción. Además de ello, quien provea una operación de interferencia, puede realizar una operación para interrumpir el sistema de apoyo de fuego del enemigo a fin de bloquear la libertad de maniobra y las fuerzas de masas en el área cercana.

Estas áreas son generalizadas tanto en espacios terrestres como cibernéticos, ya que los componentes del conflicto contienen las mismas intenciones

independientemente de la forma o teatro de operaciones a utilizar: destruir y debilitar a su oponente (Lucero, 2014). Estas pueden retrasar el tiempo de llegada de las fuerzas o capacidades enemigas o alterar la capacidad del enemigo para proyectar fuerzas o capacidades. Cuando las operaciones retrasan al enemigo, las fuerzas amigas ganan tiempo para continuar con las actividades de preparación en el área cercana. Aquí puede usarse el tiempo adicional para reconstituir, reforzar, reabastecer o maniobrar las fuerzas según sea necesario, buscando establecer las condiciones necesarias para el éxito en el cierre.

Si bien, las operaciones de interferencia no funcionarían sin las capacidades, tareas y estrategias de la inteligencia, no solo son la base de las políticas estatales, pues siempre han tenido un papel importante en la información y el ejercicio de acciones que no son ampliamente apreciadas. Aquí, las agencias de inteligencia no solo se involucran en una actividad bastante pasiva de recopilar información sobre los asuntos mundiales, sino que también intentan intervenir de manera encubierta para influir en los eventos que permitan la no materialización de los factores de inestabilidad de las naciones. En efecto, este tipo de operaciones logra percibirse como esencial para la inteligencia, y, al ser dependientes, efectivamente cuentan con el respaldo operativo y seguro que un tomador de decisiones necesita para su actuación.

Conclusiones

La actual revolución de la tecnología y la información y la globalización han posicionado la inteligencia como un factor importante para lograr una seguridad nacional adecuada frente a las amenazas militares y terroristas, entendiendo que la inteligencia es el centro de gravedad de las operaciones de interferencia. El conocimiento de alta calidad de las capacidades e intenciones de los rivales es un factor importante para lograr unos resultados equilibrados, generando así capacidades de disuasión significativas y éxito en situaciones de guerra tanto internas como externas.

Por otro lado, es importante resaltar que la aplicación de operaciones de interferencia permite obtener la superioridad de la información, situación que depende de forma prioritaria ante la calidad del capital humano. En efecto, las características del capital humano, la innovación y el pensamiento innovador son los factores clave para el éxito y la eficacia de las actividades de interferencia. Además, la mayor parte de la inteligencia relevante no puede comprarse,

más bien, tiene que ser de fabricación casera, ya que se relaciona con los rivales y las necesidades particulares del país. Por lo tanto, cada país tiene que invertir sus propios recursos para acceder al conocimiento necesario para operaciones efectivas, es decir, cada Estado tiene que formar y proyectar sus capacidades internas para recolectar, analizar y distribuir los datos necesarios en el momento relevante.

Finalmente, es posible afirmar que los principales beneficios de las operaciones de interferencia pueden clasificarse en tres puntos principales: 1. El efecto de evaluación; 2. El efecto operativo, y 3. El efecto relativo. Estos tres puntos, en primer lugar, logran ajustarse cuando un formulador de políticas planifica su presupuesto nacional y su capacidad bélica en función de su evaluación de las capacidades e intenciones del rival, lo que permite algunos márgenes de nivel de confianza. Ante ello, la aplicación de las tareas de interferencia reduce el nivel de incertidumbre al evaluar las capacidades e intenciones tácticas y estratégicas del rival. Es probable que un conocimiento más preciso de la capacidad y las intenciones del rival conduzca a un proceso más eficiente de planificación y desarrollo de la propia capacidad del país y, por lo tanto, a un mayor nivel de seguridad.

Referencias

Abad, R. M. (2014). Shalom África. Israel y Sudáfrica; las amistades peligrosas. *Historia Digital, 14*(23), 52-58.

Aguiló Bonet, A. J. (2009). El concepto de poder en la teoría política contrahegemónica de Boaventura de Sousa Santos: una aproximación analítico-crítica. *Nómadas. Critical Journal of Social and Juridical Sciences, 24*(4).

Algaba, E., Bilbao, J. M., & Fernández, J. R. (2005). *El poder de las naciones en la Unión Europea* (E2005/26). Centro de Estudios Andaluces.

Almaraz C., L. (2016). Operaciones encubiertas, su obscuridad legal: Figura vulnerante de las garantías de certeza y de seguridad jurídica. Derecho global. *Estudios sobre derecho y justicia, 1*(2), 147-170.

Almazán, J. A. (2015). Poder y Seguridad Nacional. *Estudios políticos (México)*, (34), 187-190.

Arciniegas, J. A. G. (2018). Estrategias de ciberguerra: Israel y Rusia. *Revista Perspectivas en Inteligencia, 10*(19), 57-69.

Anabalón, J., & Donders, E. (2014). Una revisión de ciberdefensa de infraestructura crítica. *Estudios Seguridad y Defensa*, (3).

Ávila, F., León, S., & Ascanio, E. N. (2013). *La frontera caliente entre Colombia y Venezuela*. Debate.

Ávila-Fuenmayor, F. (2006). El concepto de poder en Michel Foucault. *Telos, 8*(2), 215-234.

Azpíroz, M. L. (2012). *Diplomacia pública: el caso de la" guerra contra el terror"* (232). Editorial UOC.

Barba, F. R. (2015). Diplomacia cultural. ¿Qué es y qué no es? *Espacios públicos, 18*(43), 33- 49.

Bar-Zohar, M., Mishal, N., & Herrera, A. (2013). *Las grandes operaciones del Mossad*. Galaxia Gutenberg.

Bedman, F. J. (2012). Open Source Intelligence. Una perspectiva israelí. *Análisis GESI*, (4), 1.

Bejarano, M. J. C. (2012). Flame: Una nueva amenaza de ciberespionaje. *Pre-bie3*, (3), 19.

Berenstein, I. (2004). *Devenir otro con otro(s): ajenidad, presencia, interferencia*. Paidós.

Buzan, B. (1991), *Introducción a los Estudios Estratégicos. Tecnología Militar y relaciones internacionales*. Ediciones Ejército.

Caballero, F. S. (2004). Pensar la guerra. Constitución imperial y modo de control informacional. Notas para una crítica de la hegemonía americana en la cultura global. *Los heraldos de acero: la propaganda de guerra y sus medios*, 12, 125.

Cancelado, H. (2010). Poder y sistema internacional: Un aporte apócrifo a las relaciones internacionales. Revista de relaciones internacionales. *Estrategia y Seguridad, 5*(1), 33-50.

Cofré, V. (2012). *La trampa (Historia de una infiltración)*. LOM ediciones.

Cordero, S. P. Q. (2018, octubre). La responsabilidad de proteger: ¿Factor de inestabilidad de la seguridad internacional? En *III Congreso Internacional de Investigación de la Red Radar Colombia*.

Cull, N. J. (2009). *Diplomacia pública: consideraciones teóricas*. SRE.

Donlo, C. M. S. F. (2013). La lucha de los servicios de inteligencia israelíes contra el terrorismo suicida palestino durante la Intifada de Al Aqsa (años 2001-2006). *Revista Enfoques: Ciencia Política y Administración Pública, 11*(18), 103-127.

Dussán, O. (2005). Seguridad y Defensa Nacional. Prolegómenos. *Derechos y Valores, 8*(15), 104-122.

Fernández, A. M. D., García, M. F. A., Pascual, R. A., Martín, R. A., Arroyo, S., Bosch, X. B., ... & Perdices, J. M. B. (2013). *Diccionario LID Inteligencia y seguridad: estructuras de inteligencia, fuentes, análisis, diseminación y operaciones encubiertas...: 1500 términos definidos, español-inglés-francés-portugués*. Centro de Publicaciones.

Fernández, I. N. (2018). La letalidad del ciberterrorismo. *Revista general de marina, 275*(1), 133-142.

Ferreira, R. G. (2006). El caso Arbenz y las acciones encubiertas de la CIA: ¿Modelo de operación propagandística? *Revista de Historia de América*, 105-130.

Fradkin, R. (2011). Reseña de "La arquitectura histórica del poder. Naciones, nacionalismos y estados en América Latina. Siglos XVIII, XIX y XX" de Antonio Escobar Ohmstede, Romana Falcón Vega y Raymond Buve (coords.). *Historia Mexicana, 61*(1), 325-332.

Francisco, L. B. (2003). La doctrina de seguridad nacional: materialización de la Guerra Fría en América del Sur. *Revista de estudios sociales*, (15), 74-87.

García, D. (2012). La "doctrina Obama", la teoría de la "guerra limitada" y la nueva política exterior de EE. UU.: ¿hacia una política neo-nixoniana? Revista UNISCI, (28), 145-153.

García M., R. A. (2017). Seguridad Informática y el *malware* [Tesis de pregado] Universidad Piloto de Colombia.

Gerstle, G., & Wolfson, L. (2000). El poder de las naciones. *Desarrollo Económico, 40*(159), 552-556.

Gruer, M. P. M. (2013). Reflexiones sobre operaciones especiales e inteligencia en el siglo XXI. Tla-Melaua. *Revista de Ciencias Sociales, 7*(34).

Gómez, A. M. (2004). Psicología del terrorismo e inteligencia contraterrorista. *Papeles del psicólogo, 25*(88), 39-47.

Gómez, A. M. (2006). Doctrina de infiltración para inteligencia contraterrorista. *Estudios en Seguridad y Defensa, 1*(1), 31-49.

González R., R. (2015). *La instrucción militar en la Escuela de Fuerzas Especiales, estrategia de Empowerment en las Fuerzas Armadas*. https://n9.cl/k31o2

Ghotme, R. (2011). La configuración del poder en el sistema internacional contemporáneo. Revista de relaciones internacionales, *Estrategia y Seguridad, 6*(1), 47-74.

Hernández S., R., Fernández C., C., & Baptista L., P. (2014). *Metodología de la Investigación* (6.a ed.). Mc Graw Hill.

Illaro, E. L. (2014). Ciberguerra, los escenarios de confrontación. *Pre-bie3*, (1), 40.

Keegan, J. (2012). I*nteligencia militar: conocer al enemigo, de Napoleón a Al Qaeda*. Turner.

Jaramillo J., M. (2007). Aplicación de conceptos para el estudio de la inestabilidad política como amenaza a la seguridad de las naciones andinas: el caso ecuatoriano. *Papel Político, 12*(2), 565-590.

Jasso L., L.C. (2017). Seguridad nacional, inteligencia militar y acceso a la información en México. URVIO, *Revista Latinoamericana de Estudios de Seguridad*, (21), 140-156.

Jordán, J. (2016). Innovación y revolución en los asuntos militares: una perspectiva no convencional. *Seguridad, Ciencia & Defensa, 2*(2), 14.

Knorr, K. E. (1981). *El poder de las naciones*. Editorial de Belgrano.

Lazar, E., & Costescu, D. N. (2018). Los ciberataques: una noción sin tipificación, pero con un futuro. *Anuario da Facultade de Dereito da Universidade da Coruña*, 22, 157-175.

León G., B. (2019). *La crisis de la diplomacia en el ocaso del «orden liberal»: Las operaciones de estabilización*. https://n9.cl/kfohz

Liebowitz, J. (2006). *Strategic intelligence: business intelligence, competitive intelligence, and knowledge management*. Auerbach Publications.

López, L. E. (2015). El agente encubierto. *Revista de Derecho de la UNED (RDUNED)*, (17), 251-286.

Luna B., A. M. (2014). *Las operaciones de mantenimiento de la paz de las organizaciones internacionales de carácter regional*. Editorial Dykinson, SL.

Matey, G. D. (2017). El papel de la inteligencia en la lucha contra el terrorismo salafista yihadista/The role of intelligence in the fight against Salafist jihadist terrorism. *Revista cidob d'afers internacionals*, 207-228.

McSherry, J. P. (2009). *Los Estados depredadores: la Operación Cóndor y la guerra encubierta en América Latina*. LOM ediciones.

Medero, G. S. (2012). La ciberguerra: los casos de Stuxnet y Anonymous. *Derecom*, (11), 124-133.

Mendoza C., P. (2020). Inteligencia y contrainteligencia militar frente a fallos y desafíos. El caso de Culiacán, México (2019). *URVIO, Revista Latinoamericana de Estudios de Seguridad*, (26), 37-56.

Mesa Delmonte, L. (2007). El conflicto bélico entre Israel y Hezballah. Nuevos retos asimétricos para la capacidad disuasiva israelí. *Estudios de Asia y África, 42*(1),207-243.

Muñoz, M. V. (2015). *La comunicación estratégica y la diplomacia de defensa en las operaciones en el exterior*. Universidad Complutense de Madrid.

Noya, J. (2005). El poder simbólico de las naciones. *Boletín Elcano*, (73), 17.

Pastor F., A. F. (2017). *Desarrollo de un sistema demo de hacking ético para Autómatas Programables industriales y SCADA*. https://n9.cl/o40te

Porras E., C. E. (2004). El poder político y el poder militar en Venezuela. *Reflexión Política, 6*(12), 40-55.

Reboledo, D. (2016). *¿Es la ciberguerra una amenaza para la seguridad internacional o una forma de drenar rivalidades con un mínimo de violencia física y pérdida de vidas?* DOI:10.2139/ssrn.2826884

Rico, D. (2008). Configuración del estado-nación en Colombia en el contexto de globalización: una reflexión desde el escenario político. *Revista de Derecho*, (29), 3-22.

Riordan, S. (2005). La nueva diplomacia. *Foreign Policy Edición Española*, (7), 1-10.

Róbalo, H. N. E. (2016). Capacidades de las fuerzas armadas para la acción militar conjunta adecuadas a los nuevos teatros de operaciones del siglo XXI. Segunda guerra del Líbano. https://n9.cl/w0ogy

Roca, X. S. (2013). Ciberseguridad, contrainteligencia y operaciones encubiertas en el programa nuclear de Irán: De la neutralización selectiva de objetivos al "cuerpo ciber" iraní. *Pre-bie3*, (3), 22.

Rodríguez, B. (2016). La participación militar occidental contra el Daesh en Libia. *Análisis GESI*, 31.

Rodríguez, R., & Jordán, J. (2015). La importancia creciente de las fuerzas de operaciones especiales en EE. UU. y su influencia en el resto de países de la OTAN. *Revista UNISCI*, (38), 107-124.

Saddiki, S. (2009). El papel de la diplomacia cultural en las relaciones internacionales. *Revista CIDOB d'afers internacionals*, 107-118.

Sáenz I., E. J. (2020). *Ciberseguridad del PLC Siemens Simatic S7-300* [Trabajo final de grado]. Universidad Pública de Navarra.

Sainz de la P., J. A. (2012). Inteligencia táctica. *Revista UNISCI*, (28), 213- 232.

Sala, L. Y. (2018). Enemigos, población y guerra psicológica. Los "saberes contrasubversivos" argentinos y su (re) apropiación por los militares guatemaltecos. *Diálogos Revista Electrónica de Historia, 19*(2), 140-169.

Sanahuja, J. A., & Verdes-Montenegro Escánez, F. J. (2014). *Seguridad y defensa en Suramérica: regionalismo, cooperación y autonomía en el marco de UNASUR*. https://n9.cl/4c0sz

San Felipe D., C. M. (2013). La lucha de los servicios de inteligencia israelíes contra el terrorismo suicida palestino durante la intifada de al AQSA (años 2001-2006). *Revista Enfoques: Ciencia Política y Administración Pública, 12*(18),103-127.

San Julián, D. (2017). *El plan represivo de la Marina argentina y la infiltración en el grupo fundador de Madres de Plaza de Mayo (1977)*. https://n9.cl/2tkxf

Sánchez H., C. (2001). La superioridad militar de Israel y la presencia occidental en oriente medio. Nómadas. *Critical Journal of Social and Juridical Sciences*, (4).

Silva, F. (2018). StuxNet–El software como herramienta de control geopolítico. *Revistapuce*.

Sohr, R. (2019). El campo de batalla ciberespacial. *Mensaje, 68*(680), 10-13.

Spielman, J. G. (2011). *Teoría de la Seguridad y Defensa en el Continente Americano. Análisis de los Casos de EE. UU. de América, Perú y Chile*. RIL editores.

Spielman, J. E. G. (2007). Seguridad hemisférica en América Latina. Alcances y proposiciones. Journal of Globalization, Competitiveness & Governability/*Revista de Globalización, Competitividad y Gobernabilidad/Revista de Globalização, Competitividade e Governabilidade, 1*(1), 88-104.

Thomas, G., & Gambolini, G. (2001). *Mossad: la historia secreta*. Suma de Letras.

Velarde, A. J. D. (2020). Acciones de inteligencia en la Operación Militar" Chavín de Huántar". *Revista Científica General José María Córdova, 18*(29), 183-209.