

Capítulo 11

Operaciones de Inteligencia y guerras en zonas gris^{*}

DOI: <https://doi.org/10.25062/9786287602809.11>

Oscar Fernando Rubio Ramírez
Jesús María Díaz Jaimes

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: Este artículo trata sobre las Operaciones de Inteligencia y guerras en la zona gris, un tema reciente en los estudios estratégicos de las nuevas guerras. En primer lugar, se delimitan los conceptos y las características que le conciernen a los términos que se van a tratar. En segundo lugar, se enmarca el conflicto o la guerra en la zona gris –de carácter ambiguo y de difícil percepción–, la cual se desarrolla en muchos países y organizaciones criminales a nivel regional y mundial. Finalmente, en tercer lugar, se analizan los retos, oportunidades, alcances operacionales y estratégicos de la Inteligencia militar en escenarios contemporáneos de guerra y conflictos de zona gris. De esta forma se buscan estrategias que generen herramientas efectivas para desarrollar este tipo de conflictos en el escenario nacional e internacional.

Palabras clave: ambigüedad; conflicto; guerra híbrida; operaciones de inteligencia; zona gris.

^{*} Este capítulo es resultado de investigación adscrito al proyecto "*Naturaleza de la guerra contemporánea. Retos y oportunidades de las Fuerzas Especiales y la Inteligencia*", adscrito al Departamento Ejército de la Escuela Superior de Guerra, inscrito en la línea de investigación "Naturaleza de la guerra, terrorismo, nuevas amenazas", que forma parte del grupo de investigación Centro de Gravedad, con código COL0104976. Los puntos de vista pertenecen a los autores y no reflejan necesariamente los de las instituciones participantes.

Oscar Fernando Rubio Ramírez

Teniente Coronel del Ejército Nacional de Colombia. Magíster en Estrategia y Geopolítica, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Diplomado en Oceanopolítica, Escuela Superior de Guerra del Ejército de Guerra Español. Profesional en Ciencias Militares, Escuela Militar de Cadetes "General José María Córdova", Colombia. Contacto: oscar.rubio@buzonejercito.mil.co

Jesús María Díaz Jaimes

Teniente Coronel (R) del Ejército Nacional de Colombia. Magíster en Estrategia y Geopolítica, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Especialista en Ciencia Política, Universidad Autónoma de Bucaramanga, y en Gerencia, Universidad Militar Nueva Granada, Colombia.

<https://orcid.org/0000-0001-6595-8277> - Contacto: jesus.diaz@esdeg.edu.co

CitaciónAPA: RubioRamírez, O.F., & Díaz Jaimes, J. M. (2024). Operaciones de Inteligencia y guerras en zonas grises. En L. A. Montero Moncada & O. A. Garzón Gómez (Eds.), *Comandos: Retos de las Fuerzas Especiales e Inteligencia en la guerra contemporánea* (pp. 257-286). Sello Editorial ESDEG. <https://doi.org/10.25062/9786287602809.11>

COMANDOS: RETOS DE LAS FUERZAS ESPECIALES E INTELIGENCIA EN LA GUERRA CONTEMPORÁNEA

ISBN impreso: 978-628-7602-79-3

ISBN digital: 978-628-7602-80-9

DOI: <https://doi.org/10.25062/9786287602809>

Colección Seguridad y Defensa

Sello Editorial ESDEG

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Bogotá D.C., Colombia

2024



Introducción

Los conflictos armados o guerras mundiales, en especial los llevados a cabo a finales del siglo XIV hasta nuestros días, han pasado por múltiples cambios en el campo de batalla. Empezando con la guerra de primera generación, que incluye las guerras europeas que libraron los ejércitos napoleónicos en el siglo XIX con el fin de conquistar o asegurar la soberanía de territorios, su característica principal fue el uso en masa de las armas de fuego en el campo de batalla hasta el siglo XX (Aznar, 2015). El uso de grandes cuerpos de ejércitos que se enfrentaban de forma directa fue aplicado en la Primera Guerra Mundial, la cual sirvió para evolucionar a nuevos conceptos, como la guerra indirecta del pensador militar Liddle Hart, quien inspiró la guerra móvil o relámpago (*blitzkrieg*) del ejército alemán en la Segunda Guerra Mundial (Del Rey & Canales, 2012). Las características más importantes de este tipo de guerra son la industrialización y la mecanización, siendo uno de sus elementos fundamentales la capacidad de movilizar grandes ejércitos y el uso de maquinaria bélica, lo cual generó nuevas tecnologías para la creación de armas y doctrinas para aplicarlas.

Asimismo, a partir de Carta de las Naciones Unidas del 26 de junio de 1945 y de los Convenios de Ginebra del 12 de agosto de 1949 (que introducen el concepto eminentemente material de *conflicto armado*), se generaron nuevas reglas y deberes que los Estados deben cumplir en caso de un conflicto entre Estados o dentro de ellos, según sea el caso (Raggio, 2019). Estas normativas marcaron los múltiples conflictos de la segunda mitad del siglo XX, en lo que se conoció como la Guerra Fría, en el cual participaron las dos superpotencias hegemónicas del momento: por un lado, la Unión de República Socialistas Soviéticas (URSS), que encarnaba el modelo comunista de desarrollo, y, por el otro, los Estados Unidos de América (EE. UU.), que lideraba el modelo capitalista-liberal. Aunque la principal

característica de este conflicto fue que no hubo confrontación armada directa entre las fuerzas militares, estas sí participaron activamente en la ampliación de sus espacios de influencia en terceros países de todos los continentes para debilitar el dominio político, económico o militar de su adversario.

Esta situación dio como resultado la intensificación de muchos conflictos internos en muchos países, entre otros en Vietnam, Nicaragua, Laos, Afganistán y el Congo, en los cuales se armaron y entrenaron muchos grupos irregulares para que tomaran el poder del Estado que confrontaban. En este escenario surgió el concepto de *guerra asimétrica*, el cual se refiere al uso de métodos no convencionales, tales como el terrorismo, la guerra política, la guerra sucia, la contrainsurgencia y la desinformación (Cuneo, 2019), pues la disparidad en la fuerza militar para atacar se compensaba con estos métodos para cumplir los objetivos políticos. Dado que estas condiciones forjaron un nuevo tipo de guerra muy difícil de afrontar por parte de los Estados en el marco del Derecho Internacional Humanitario (DIH), se violaron muchos Derechos Humanos y se crearon o consolidaron varias dictaduras de diferente corte en el mundo durante la Guerra Fría.

Cuando la URSS colapsó en 1991 ante el fracaso de su modelo económico y político, se desencadenó la desintegración de los Estados que la conformaban, en especial los del este de Europa, y la pérdida de su área de injerencia en varias partes del mundo. Esto dio paso a una nueva era de conflictos internos y al auge de grupos radicales religiosos musulmanes, los cuales generaron la mayor acción terrorista a comienzos del siglo XXI: impactaron dos aviones comerciales en las Torres Gemelas en la ciudad de New York. Este ataque tuvo como resultado una nueva guerra, esta vez contra el terrorismo, que fue liderada por el gobierno Bush (Correa, 2017).

Como represalia, el gobierno de los Estados Unidos intervino directamente en varios países para atacar a las células militares de los grupos armados que utilizan el terrorismo islámico, denominados yihadistas; este es el caso de Al Qaeda, que tenía su base de entrenamiento en Afganistán o en Iraq para derrocar al dictador Saddam Husein. Estas guerras dieron como resultado un incremento considerable en la afectación a la población civil debido al uso indiscriminado de acciones terroristas, como vehículos bomba y ataques suicidas, tácticas difíciles de contrarrestar por un ejército regular.

Como consecuencia de la caótica situación de seguridad y debido a la proliferación de múltiples grupos irregulares en Iraq, después de la invasión de los Estados Unidos surgió en 2014 el grupo yihadista Daesh, el autodenominado

Estado Islámico o también conocido como ISIS o ISIL, que profesan la rama más tradicional y ortodoxa del islam, la suni, grupo que desplazó de la escena a Al Qaeda y Al Nusra (Muñoz, 2018). Esto generó una confrontación directa contra los ejércitos iraquí y sirio, la cual resultó en la apropiación de bastas áreas de cada país y en la proclamación de un nuevo califato.

Las consecuencias de estos hechos desembocaron en una guerra regional de gran escala en la península arábiga, en la cual el uso de los medios de comunicación y las redes sociales adquirieron un nuevo papel, pues estas herramientas fueron indispensables en el reclutamiento y la expansión de su ideología en todo el mundo. Como resultado se produjeron múltiples ataques terroristas en Europa y los Estados Unidos por parte de los denominados *lobos solitarios* (Cuneo, 2019), que son personas reclutadas por medio de redes sociales para ejecutar ataques terroristas de resonancia y así posicionar el grupo en la escena mundial. Sin embargo, gracias a la campaña militar que realizaron las fuerzas de la Organización del Tratado del Atlántico Norte (OTAN), Rusia e Irán, las cuales apoyaron a las autoridades locales de Iraq y Siria con ayuda militar y financiera, se logró en 2017 derrotar militarmente a Daesh, de tal manera que estas fuerzas pudieron mantener sus intereses estratégicos en la región.

Ahora bien, respecto al entorno regional del continente americano, se debe señalar que en sus hemisferios centro y sur existen grupos armados que utilizan métodos y acciones de carácter terrorista para cumplir sus fines, como sucede en México con los Zetas o el cartel de Sinaloa. Dichos grupos narcotraficantes cuentan con un gran poder económico que obtuvieron con el tráfico de estupefacientes, han construido grandes ejércitos con arsenal militar proveniente de los Estados Unidos y tienen un control total en algunos Estados donde son ley.

Por medio de la intimidación y los asesinatos selectivos, estos grupos logran efectuar cogobierno y participan activamente en el desarrollo de las políticas regionales (Zavala, 2018) para cumplir sus propios intereses. Frente a esta situación, el Estado mexicano, en cabeza de sus Fuerzas Armadas, ha dado una lucha frontal contra estas organizaciones y ha fortalecido su capacidad operativa y de inteligencia, lo cual dio como resultado en el año 2016 la captura del líder del cartel de Sinaloa conocido con el alias del *Chapo Guzmán*.

Respecto a Colombia, se identifican varios grupos armados, algunos con más de cincuenta años de existencia, como es el caso del Ejército de Liberación Nacional (ELN). Otros grupos se formaron a partir de las desmovilizaciones de antiguas agrupaciones armadas, por ejemplo el Clan del Golfo, que absorbió a

algunos antiguos integrantes de las Autodefensas Unidas de Colombia (AUC) y sus áreas de injerencia (Bolaños, 2018). Otro ejemplo tuvo lugar con el proceso de paz entre el Gobierno colombiano y las Fuerzas Armadas Revolucionarias de Colombia (FARC), que derivó en el surgimiento de varias facciones o grupos, como las FARC Residual, La Segunda Marquetalia y los Comandos de Frontera.

En este escenario, las Operaciones de Inteligencia han sido la punta de lanza de todos los organismos de inteligencia del Estado para dismantelar dichas organizaciones, donde el ingenio y el uso del engaño son importantes. A modo de ejemplo, se puede mencionar la operación “Jaque”, desarrollada el 2 de julio del 2018, en la que los miembros de la Inteligencia militar usaron una fachada e historia ficticias para hacerse pasar por una organización no gubernamental (ONG) que, aparentemente, recogería a quince secuestrados que tenían las FARC, entre ellos la excandidata presidencial Ingrid Betancourt, secuestrada desde 2002 (Bolaños, 2018). Estas personas fueron liberadas después de que abordaran un helicóptero que, supuestamente, los llevaría adonde se encontraba Guillermo León Sáenz Vargas, alias *Alfonso Cano*, cabecilla principal de la organización en esa época. Durante esta operación fueron capturados dos cabecillas del Frente Primero, Gerardo Aguilar, alias *César*, y Alexander Farfán, alias *Enrique Gafas*, sin efectuar disparo alguno.

Cabe señalar que esta Operación de Inteligencia es un referente mundial del modo como se pueden obtener resultados operacionales estratégicos y de alto impacto nacional sin recurrir al uso de armas de fuego. La principal lección es que el conocimiento y el análisis de la manera como opera o delinque una organización, grupo criminal o fuerza enemiga que se quiere atacar, permite bloquear sus fortalezas y explotar al máximo las debilidades para conseguir los objetivos que se persiguen.

Debido a esto, las Fuerzas Militares y de Policía colombianas han pasado por un proceso de transformación en su capacitación y doctrina para contrarrestar las múltiples amenazas que enfrentan. En este contexto, las Operaciones de Inteligencia se refieren a las tareas que realizan las unidades de Inteligencia militar y unidades de combate para obtener información que contenga las respuestas sobre los requerimientos críticos del comandante (Schachtner, 2018). Específicamente, el personal de la especialidad de Inteligencia es el encargado de planear y ejecutar las Operaciones de Inteligencia contra las amenazas y grupos armados que delinquen en sus áreas de operaciones.

En resumen, la guerra se ha transformado acorde con el desarrollo humano en un mundo globalizado. La naturaleza de los conflictos ha experimentado muchos cambios, especialmente al final de la Guerra Fría, de manera que no es común observar conflictos entre ejércitos de Estados-naciones, con la excepción de la guerra actual entre Rusia y Ucrania, ya que las confrontaciones armadas se han enfocado en guerras internas o civiles, así como en la creación de grupos radicales que buscan cumplir sus objetivos o fines políticos por medio de métodos no convencionales, entre los cuales se encuentra el terrorismo. Estas características generan un espectro no físico llamado la *zona gris*.

En este espectro de guerra en zona gris prevalecen las acciones políticas, económicas, jurídicas, convencionales y no convencionales que, a la postre, buscan socavar el ímpetu o deseo de confrontación del adversario para que cumpla con los deseos u objetivos del Estado. En este contexto, lo más importante es que no se comprometa de forma directa el actuar de las fuerzas regulares de la nación, que es lo que llevaría a escalar en una tensión diplomática o, en el peor de los escenarios, una confrontación bélica.

Conceptos “Operación de Inteligencia” y “zona gris” dentro del desarrollo de las guerras contemporáneas

Operación de Inteligencia

La inteligencia, según la definición de la OTAN, en un sentido amplio y dentro del contexto militar, es el resultado de la integración e interpretación de nuestros conocimientos sobre el terreno, la meteorología, las actividades, las capacidades y/o las intenciones de un enemigo actual o potencial (Sainz, 1991). Tiene la intención de comprender o entender el comportamiento de la amenaza para obtener un conocimiento amplio y profundo del modo como actúa o delinque. También se considera como una disciplina que sigue un proceso lógico, una secuencia de pasos que conducen a un producto o una información final que pueda servir al mando operacional para la toma de decisiones.

En este sentido, una Operación de Inteligencia incluye las tareas o acciones efectuadas por personal capacitado y entrenado en recolectar información del enemigo o amenaza, la cual varía según la doctrina militar del país (Quiñónez, 2012).

Normalmente, los conceptos se desarrollan con base en las experiencias que haya tenido en las diferentes guerras en que esté inmerso y en el tipo de guerra, ya sea convencional o irregular/no convencional. Vale la pena mencionar que estas actividades son planeadas y ejecutadas por personal entrenado y capacitado para dichas misiones, quienes son conocidos como agentes de inteligencia y que deben cumplir unos requisitos y condiciones especiales para cumplir estas tareas, que son designadas por las autoridades pertinentes de un Estado o nación.

Los agentes de inteligencia cuentan con un perfil definido, así como con unas características físicas y psicológicas que se adaptan al entorno o las circunstancias en las que se desea operar. Estos agentes deben ser capaces de efectuar el ciclo de inteligencia, especialmente en el planeamiento y la recolección de información, para así generar un análisis y uso de la información de forma óptima y de acuerdo con los objetivos y alcances que se desean en la Operación de Inteligencia. La mayoría de los agentes secretos son hombres callados y muy discretos, capaces de infiltrar sin mayor sospecha altos círculos diplomáticos, gubernamentales o empresariales (Swenson & Sancho, 2015), pues se saben mimetizar utilizando hábilmente una fachada o historia ficticia que les facilita y genera una seguridad para no ser descubiertos por el enemigo.

Asimismo, existen al menos tres grandes necesidades que se cubren con los diferentes tipos de inteligencia: la inteligencia militar, la inteligencia estratégica y la información policial o criminal (Swenson & Sancho, 2015). Según el caso, los agentes efectúan actividades u Operaciones de Inteligencia para prevenir, detectar y neutralizar amenazas o delitos que existen en el entorno de seguridad y defensa de un país, los cuales pueden cambiar en función de los intereses nacionales y geopolíticos que enfrentan en cualquiera de los dominios, ya sea de carácter terrestre, marítimo, aéreo, cibernético, logístico o biológico (Méndez et al., 2019).

En este contexto, las Operaciones de Inteligencia se desarrollan de acuerdo con las necesidades o vacíos de información que requiere el mando para planear sus operaciones. Como se detalla en los siguientes apartados, las Operaciones de Inteligencia se clasifican de en espionaje, sabotaje, decepción, psicológicas, información y neutralización.

Espionaje

Es la tarea principal de cualquier agencia de inteligencia desde la concepción de los antiguos Estados, los cuales la efectuaban para recopilar información de las capacidades y debilidades de los Estados rivales y, a partir de allí, planear sus ataques.

El espionaje es una actividad encubierta que se realiza para obtener información clasificada mediante el empleo de espías, para beneficio de una organización o de un Estado, por lo cual el espía debe ser un individuo de gran preparación y altamente adiestrado para obtener información clasificada de carácter político, económico, psicosocial o militar utilizando procedimientos clandestinos o encubiertos (Llop et al., 2013).

Según Gamboa (2016), el viejo concepto de *inteligencia/espionaje*, que se centraba en las meras tareas informativas sobre “lo secreto”, hace tiempo que fue superado para dar paso a otro de horizonte mucho más abierto y que exige una mayor integración con el objetivo de realizar nuevas y complejas tareas, desarrollarlas con fundamento científico y adaptarlas a la obtención y tratamiento de la información procedente de nuevos y numerosos ámbitos (Gamboa, 2016).

Asimismo, de acuerdo con sus necesidades y la misión asignada, el espionaje explota diferentes fuentes de información, como el reclutamiento de personas que tengan acceso a información, la documentación de interés, la transmisión técnica de información, las actividades propias del agente o espía, la infraestructura física para efectuar las actividades de inteligencia, el material o el equipo y el ambiente natural, que es el estudio del entorno físico donde se ejecutan las actividades de espionaje (Llop et al., 2013).

Con la globalización de la información por medio del internet, es muy fácil acceder a múltiples “fuentes abiertas” (OSINT, por la sigla en inglés de Open Source INtelligence), las cuales proporcionan grandes volúmenes de datos que son difíciles de seleccionar, contrastar y analizar adecuadamente. Por ello se hace necesario el uso amplio de las nuevas tecnologías que puedan ayudar en la búsqueda y el rastreo de información de interés nacional.

Las agencias de inteligencia avanzadas del mundo se han adaptado al nuevo escenario internacional globalizado y aprovechan ahora las posibilidades que ofrecen las tecnologías de la información y la comunicación (TIC). Finalmente, cabe señalar que las agresiones por parte de Estados, grupos o individuos con la finalidad de lograr información que les permita obtener ventajas estratégicas, políticas o económicas, han sido una constante histórica y siguen siendo una amenaza de primer orden para la seguridad (Gamboa, 2016).

Sabotaje

También conocida como *subversión*, es el conjunto de acciones encubiertas de violencia física realizada contra los bienes materiales, sean estos de propiedad

individual, colectiva o pública; estas acciones van desde la simple alteración de la función que cumple hasta su destrucción total (Llop et al., 2013). En un contexto general, la finalidad del sabotaje es desestabilizar al Estado en cualquiera de sus ámbitos, bien sea económico, político, social o militar, para obtener ventajas tácticas que a la postre tendrían consecuencias estratégicas a favor.

Esta actividad va ligada a la ejecución de operaciones militares que, en una guerra convencional, buscan cumplir los objetivos que el Estado ha definido contra la amenaza o enemigo; es decir, a diferencia de la guerra no convencional, no necesariamente se realizan operaciones militares para afectar al enemigo y cumplir los objetivos. La ejecución de cualquier acción de sabotaje requiere de informaciones para tener un conocimiento de las características específicas y técnicas del objetivo por sabotear, de manera que el enemigo o adversario externo o interno orientará sus esfuerzos para satisfacer estas necesidades de información (Llop et al., 2013).

Los objetivos que se pueden cumplir con el sabotaje dependen de la capacidad del Estado u organización en acceder a los bienes materiales o redes informáticas del enemigo, pues de esto depende que tenga las condiciones para afectar la documentación importante, la infraestructura crítica, el material y el equipo de las fuerzas armadas enemigas, la infraestructura informática o páginas web de las instituciones gubernamentales, y el ambiente natural o geográfico que puedan generar una ventaja táctica o estratégica (Llop et al., 2013). Con este propósito se utiliza la modalidad de sabotaje incendiario, es decir, el sabotaje con explosivos utilizado especialmente contra infraestructura crítica; el sabotaje mecánico contra los equipos y las capacidades militares enemigas, y, el más utilizado en la actualidad, el sabotaje informático para robar información, impedir o neutralizar el funcionamiento de los sistemas informáticos de la amenaza.

Decepción

Las operaciones de decepción se usan para efectuar un engaño militar o desinformación, que según Andrade et al. (2011) son las acciones ejecutadas con el objetivo de engañar a los adversarios sobre las capacidades, intenciones y operaciones de las fuerzas militares propias, promoviendo un análisis equivocado y causando que el adversario obtenga conclusiones falsas. De esta manera se búsqueda obtener una ventaja en las operaciones militares o de inteligencia y minimizar los efectos adversos de las acciones enemigas sobre los intereses nacionales.

Además, otro objetivo de las operaciones de decepción es erosionar la credibilidad de las personas u organizaciones adversarias en su toma de decisiones

manipulando su percepción de realidad. Con ello se busca ganar tiempo y resquebrajar la unidad de mando militar o la política del adversario, pero sin comprometer una gran cantidad de tropas o equipos militares para obtener ventajas estratégicas. En el ámbito de las Operaciones de Inteligencia, este tipo de operaciones de decepción se aplica en el campo de la inteligencia humana y técnica, así como en las comunicaciones enemigas y en su estructura informática.

Psicológicas

Hacen referencia a la estrategia planeada y dirigida para utilizar un conjunto de elementos, como la propaganda, los medios de comunicación y otras formas de acción psicológica –empleados por cualquiera de las fuerzas en conflicto–, con el propósito de influir en la voluntad, la actitud y el comportamiento de las tropas, los grupos de población y los miembros de las organizaciones hostiles (Andrade et al., 2011) para buscar ventajas estratégicas y lograr el éxito en el desarrollo de la guerra.

Dado que las operaciones psicológicas están encaminadas a brindar apoyo a las operaciones militares, no pueden ser ejecutadas por fuerzas independientes. Específicamente, se dividen en tres categorías: de carácter estratégico, táctico y de consolidación, dependiendo de las características geográficas del ambiente operacional, el blanco audiencia que se quiere impactar y el tiempo estimado para su ejecución. Por ende, las operaciones psicológicas de consolidación se desarrollan en áreas en las cuales ya existe control por parte del Estado, que busca generar una normalidad y apoyo de la población civil.

En este sentido, se hace necesario el uso de tecnología de vanguardia con capacidad de penetrar los medios de comunicación enemigos, bien sea de forma directa o indirecta, para generar la matriz de opinión o percepción de acuerdo con los objetivos establecidos y obligando al adversario a pelear en nuestro campo de información o desinformación, lo cual daría un resultado en el campo táctico o estratégico positivo según los objetivos planteados para la misión.

Asimismo, existen numerosos métodos que se pueden emplear en las operaciones psicológicas, dependiendo de los múltiples factores y las categorías que se utilicen, como los sistemas de transmisión de radio y televisión; la distribución por aire de material impreso o panfletos, obsequios y otros útiles; campañas de rumores contra el adversario; publicar derrotas militares enemigas; escasez de alimentos, falta de alojamiento, ropa o cualquiera de los artículos de primera necesidad; fraccionamiento y falta de confianza interna; conflictos por la administración y manejo de recursos económicos (Andrade et al., 2011), y, en general, cualquier debilidad en el sistema enemigo que ayude a diezmar su voluntad de lucha.

Información

Son las actividades de Inteligencia encaminadas a usar la información para cumplir los objetivos nacionales. Como la diplomacia, la competencia económica o el uso de la fuerza militar, la información por sí misma es un aspecto esencial del poder nacional (Andrade et al., 2011); en todo caso, estas pueden ser utilizadas de forma simultánea en operaciones defensivas y ofensivas para cumplir con la misión, así como para proteger las capacidades propias y atacar sistemáticamente a la amenaza.

Para ello se utilizan todos los medios de difusión de información con los que se cuentan: radio, televisión, medios escritos, redes sociales y medios digitales. Además, se debe cumplir con unos criterios de calidad de la información que están relacionados con la exactitud, la relevancia, el sentido del tiempo, el valor práctico, la información completa, la brevedad y la seguridad, con el fin de obtener un producto informático óptimo para usarlo con el blanco audiencia que se quiere desinformar o fortalecer, según sea el caso.

Los objetivos de las operaciones de información son amplios y de gran alcance, ya que actualmente la sociedad se encuentra hiperconectada por los medios digitales y las redes sociales. Por ende, los agentes de inteligencia deben estudiar y planificar para influir exitosamente sobre el blanco audiencia elegido, explotando sus emociones, motivos y razonamiento objetivo, así como el comportamiento de sus gobiernos, organizaciones, grupos e individuos (Andrade et al., 2011), con el fin de destruir, interrumpir o negar el uso de la información del adversario, además de degradar, engañar, explotar, influir, proteger, detectar, restaurar o responder cualquier información enemiga que afecte la credibilidad de las instituciones, personas u organizaciones propias.

Neutralización

Las operaciones de neutralización son aquellas que van encaminadas a anticipar cualquier acción bélica o no armada que pueda afectar la integridad o las instituciones de un Estado u organización. De esta manera, se busca contrarrestar las intenciones, amenazas y objetivos de los adversarios o enemigos mediante la “contrainteligencia” (Quiñónez, 2012), para afectar la capacidad de mando y control del adversario, por ejemplo, liquidando los comandantes de las unidades enemigas con métodos no convencionales u operaciones militares con unidades de Fuerzas Especiales.

También se busca afectar la capacidad logística o económica de la amenaza atacando su infraestructura crítica y, sobre todo, las figuras políticas o militares

enemigas beligerantes. Como ejemplo se puede mencionar la operación que realizaron los Estados Unidos en el año 2020 para matar al general iraní Qasem Soleimani, comandante en jefe de las fuerzas Quods en Irak, quien era visto como una posible amenaza a la seguridad o legitimidad de dicha nación.

De esta manera, se concluye que las Operaciones de Inteligencia no solo deben dirigirse contra las amenazas directas, pues si bien el espionaje proporciona las informaciones o insumos necesarios para prevenir, detectar y neutralizar una amenaza, también da los argumentos necesarios para efectuar planeamiento prospectivo sobre los posibles cambios en el ámbito político, económico, militar o social que puedan afectar los intereses nacionales o estratégicos del Estado.

Zona gris

El concepto de zona gris fue acuñado recientemente por académicos en geopolítica y desarrollado por algunos Estados, que lo definen como un espectro o un nuevo teatro de la guerra no convencional, de carácter ambiguo, que no cuenta con un espacio físico definido. Sin embargo, se debe señalar que algunos actores no reconocen esta zona ni la delimitan en el análisis estratégico que hacen sobre su seguridad, pues dado que su estrategia cuenta con varias dimensiones y aristas, se dificulta que creen una estrategia general rígida. Además, si la pusieran en práctica, no generará en algunos casos el objetivo final en corto tiempo (Jordán, 2018), de manera que los métodos y las técnicas para poder atacar los diferentes elementos que existen en la zona gris se deben generar de forma gradual y concisa.

Características de la zona gris

La zona gris hace referencia a un concepto amplio y con unas características difíciles de percibir a primera vista, pero que las naciones y las organizaciones criminales desarrollan para cumplir sus objetivos estratégicos. Específicamente, este espectro cuenta con cuatro características: ambigüedad, gradualismo, intereses sustanciales en juego y estrategias multidimensionales, las cuales se describen en los siguientes apartados.

Ambigüedad

Se refiere a que no se plantean relaciones pacíficas ni conflicto armado. En el conflicto en la zona gris, la competición estratégica entre dos o más Estados (con sus respectivas diadas conflictivas) discurre por debajo del umbral de violencia política del conflicto armado menor (Baqués, 2017). Es decir, una confrontación a pequeña

escala, donde pueden existir reclamos verbales, protestas y utilización de la población civil en contra de las autoridades, lo cual puede generar una disputa política a lo largo del tiempo.

En esta característica también tienen un papel las Fuerzas Militares, que pueden efectuar ejercicios disuasorios o de demostración de fuerza en las áreas de confrontación o en las fronteras entre naciones, pero evitando que se escale a un conflicto armado abierto. A modo de ejemplo vale la pena mencionar el envío de aviones de combate de la Fuerza del Aire de la República Popular de China sobre las aguas territoriales de Taiwán; este caso muestra que se procura no cruzar líneas rojas que puedan desembocar en una contienda militar con costes muy elevados y consecuencias imprevisibles (Mazarr, 2015). En este sentido, para el Estado más fuerte tiene un papel importante conocer la capacidad de respuesta de su adversario para evitar una contestación de carácter bélico más fuerte y amplia, la cual se puede tornar en una guerra directa que salga del espectro de la zona gris.

Esta ambigüedad intencionada dificulta tanto la identificación de las actividades hostiles propias de la zona gris, como la articulación de estrategias de respuesta (Mazarr, 2015). Por esta razón, para las agencias de Inteligencia y la estrategia general es importante saber los objetivos políticos que persigue la amenaza y los medios con los que cuenta para atacar en la zona gris, de manera que pueda prevenir, detectar y, en lo posible, neutralizar las intenciones o disminuir las consecuencias de las acciones enemigas.

Gradualismo

El gradualismo refuerza la ambigüedad, pues la gravedad última y la interrelación de las distintas acciones no siempre resultan obvias a los decisores políticos del rival, a sus aliados ni a sus respectivas opiniones públicas (Mazarr, 2015), en un contexto en el que el tiempo no puede ser definido y los resultados o progresos que se quieren lograr suceden de forma lenta o paulatina. Además, esa gradualidad hace que se establezca un *statu quo* en las acciones que poco a poco va generando cambios o modificaciones en el conflicto de zona gris, lo cual puede crear un nuevo escenario de guerra híbrida o directa, según sea el caso, o, por el contrario, producir un hecho consumado que permita cumplir el objetivo estratégico.

Intereses sustanciales en juego

Esta característica de la guerra en zona gris es el motivo por el cual se genera el conflicto, ya que los intereses y beneficios que se quieren lograr son mayores a los riesgos que se corren si el enemigo o la amenaza los descubre. Es decir, en este

escenario se abandona la vía diplomática tradicional para adoptar estrategias que podrían cruzar líneas rojas, lo cual, de ser descubierto, podría acarrear sanciones o problemas diplomáticos graves para la nación, dependiendo de su peso geopolítico en el conflicto y de las alianzas que tenga con actores que puedan respaldarlo.

El efecto de la asimetría de intereses también se aprecia fuera de la zona gris, puntualmente en conflictos armados donde el débil vence al fuerte por razones similares (Mack, 1975). Asimismo, en la zona gris los intereses pueden ser antagónicos, por lo cual la respuesta por parte de las alianzas dependerá de si la amenaza los afecta de forma directa o si solo es un conflicto entre dos partes, por lo cual evitarán escalar el conflicto y procurarán ser neutrales para cuidar sus intereses nacionales.

Estrategias multidimensionales

Se puede decir que la guerra en zona gris tiene una gama de acciones o estrategias que se adaptan de acuerdo al tipo de guerra y los objetivos que se quieren cumplir. Específicamente, en este contexto las acciones pueden tener similitudes con la estrategia utilizada en la guerra híbrida, la cual ha incorporado un rango de diferentes modos de combatir, como "las capacidades convencionales, las formaciones y tácticas irregulares, los actos terroristas, incluyendo la violencia indiscriminada, la coerción y el desorden criminal" (Hoffman, 2007, p. 132). Todas estas acciones, que pueden ocurrir de forma "simultánea y adaptativa", se definen en un tipo de guerra multimodal utilizada y aprovechada por "Estados o grupos que seleccionan de todo el menú de tácticas y tecnologías y las mezclan de manera innovadora para encontrar su propia cultura estratégica, geografía y objetivos" (Hoffman, 2009, p. 5).

Se puede concluir que la guerra o el conflicto en la zona gris consiste en el empleo intencionado, multidimensional e integrado de diversos instrumentos de poder: políticos, económicos, sociales, informacionales, diplomáticos y también militares (Mazarr, 2015). En este escenario, la fuerza militar se usa de forma simbólica, con intención coercitiva, es decir, con el fin de señalar, intimidar y marcar territorio, o, en algunos casos, para respaldar a otros actores que están ejerciendo la fuerza. Sin embargo, se debe enfatizar en que la característica fundamental del conflicto en la zona gris es el empleo amplio e integrado de herramientas no armadas, pues si se emplea la fuerza militar para efectuar acciones ofensivas, el conflicto habrá escalado a una guerra abierta y directa, de modo que ya no se podría hablar del espectro de zona gris.

Dado que estas cuatro características son esenciales para determinar si existe un conflicto en zona gris, para la mayoría de la población civil es difícil determinar que existe un conflicto contra una amenaza que podría desestabilizar su estilo de

vida. Por lo tanto, buscar el apoyo de la opinión pública para legitimar los métodos o medios para atacar una amenaza o enemigo resulta ser una ardua tarea, de manera que es más práctico establecer alianzas regionales que comulguen con los mismos principios u objetivos para atacar dichas amenazas, pues, como dijo Waltz (2010), el sistema internacional se encuentra determinado por dos factores: el primero es la anarquía internacional, que es ausencia de una autoridad supranacional que garantice de manera efectiva la seguridad de los Estados, y el segundo es la distribución de poder relativo entre los Estados (Waltz, 2010).

Importancia operacional y estratégica de la Inteligencia militar en escenarios contemporáneos de guerra y conflictos de zona gris a nivel mundial y regional

Es importante tener clara la naturaleza del conflicto y de los actores que participan, ya que los procedimientos suelen cambiar dependiendo del impacto que se quiera obtener, bien sea a nivel táctico, operacional o estratégico, y de acuerdo con las directrices o intenciones del conductor de la guerra, quien sería el presidente o líder de la nación. En este escenario, las Operaciones de Inteligencia pueden obtener resultados estratégicos y de gran impacto nacional sin utilizar necesariamente un componente militar armado en su planeamiento o ejecución, de tal modo que se puedan evitar los riesgos de una confrontación armada, que sería mucho más grave en una guerra convencional entre dos o más países.

Por ende, la Inteligencia militar tiene un papel fundamental en el desarrollo de las guerras convencionales y no convencionales –en especial en la guerra en zona gris–, ya que las Operaciones de Inteligencia la proveen con las herramientas necesarias para recolectar la información, ya sea de carácter operacional o estratégico, que no solo ayuda a prevenir las intenciones o amenazas del adversario, sino que además brinda los insumos necesarios para planear las estrategias adecuadas a las capacidades enemigas y el ambiente operacional y estratégico en que está inmerso el conflicto.

Ahora bien, también se debe señalar que existe un elemento importante sobre la intencionalidad tramposa o fraudulenta en las acciones que efectúa el actor en la guerra de zona gris, ya que va en contravía del principio de buena fe que profesan los Estados en las relaciones internacionales (Baqués, 2017). Por ende, las

Operaciones de Inteligencia que se ejecutan en la zona gris deben tener un carácter de compartimentación y secreto operacional, lo cual restringe las posibilidades de que se transgredan los límites permitidos en esta zona y generar problemas que puedan escalar a un conflicto directo con el adversario.

En este punto ya se ha señalado a autores como Baqués (2017) o Jordán (2018), quienes se refieren explícitamente a la contravención del principio de la buena fe que debe regir en las relaciones internacionales como uno de los elementos relevantes del concepto. Así las cosas, las actuaciones en zona gris, si bien tratan de evitar a toda costa traspasar los límites establecidos, no pueden catalogarse como manifestaciones ordinarias, regulares y legítimas de las relaciones internacionales porque, precisamente, transgreden el principio de buena fe que las define.

Oportunidades en el uso de las Operaciones de Inteligencia y su aplicación en zonas grises en el desarrollo de las guerras contemporáneas

El conflicto o guerra en zona gris abre un abanico de posibilidades para efectuar Operaciones de Inteligencia acordes con la capacidad y el entrenamiento de las agencias de inteligencia. Asimismo, el factor económico desempeña un papel importante, pues no importa el tipo de operación que se quiera ejecutar, los recursos económicos determinan la duración y la continuidad de la actividad de inteligencia.

Específicamente, existen múltiples oportunidades o mecanismos que se pueden emplear en la zona gris, algunos de los cuales se presentan en los siguientes apartados.

Operaciones de influencia sobre la opinión pública del adversario y sobre la opinión pública internacional

Estas acciones se pueden enmarcar en las Operaciones de Inteligencia psicológicas o de información, en las cuales se crean o construyen narrativas que se puedan difundir a través de los medios de comunicación propios o del enemigo. De esta manera, se crean noticias o mensajes que fortalecen el punto de vista propio y se difama de la narrativa del adversario, para lo cual es importante emplear todos los tipos de redes sociales que puedan ser usados por el público o la audiencia objetivo.

En la actualidad existen varias empresas que generan tendencias en las redes sociales por medio de bodegas web o de información, en las cuales varias

personas utilizan computadores con múltiples perfiles falsos en las distintas plataformas, como Facebook, Twitter (ahora X), TikTok e Instagram, para posicionar de forma coordinada alguna tendencia o información de acuerdo con las necesidades del solicitante. Estas bodegas, también llamadas “granjas de *trolls* y de *clicks*”, comunes en algunos países, especialmente en Rusia, han afectado procesos electorales en Europa y los Estados Unidos. Con este propósito, también utilizan las *fake news* o noticias falsas, muy frecuentes en las redes sociales, lo que algunos ya denominan *deep fake*, e incluso podrían alterar videos muy creíbles para hacer que alguien diga y haga lo que necesitan (Marín, 2020). Estas herramientas son importantes, junto con la inteligencia artificial, para generar contenido informático creíble y de fácil entendimiento que genere la matriz de opinión favorable a nuestros intereses.

Asimismo, en el contexto regional deben existir medios de comunicación robustos y de buena reputación que puedan servir de caja de resonancia a las informaciones o noticias que se busca difundir, de manera que no se deben utilizar muchas *fake news* que puedan dañar su prestigio. En este sentido, la narrativa debe ser coherente con hechos reales que sean difíciles de refutar por parte de la contraparte. Finalmente, se debe tener en cuenta que en las áreas apartadas, donde no existe una influencia fuerte de los medios de comunicación escritos o digitales, la información llega por medio de mensajes de texto o cadenas de aplicaciones de mensajería instantánea.

En este contexto, aplicaciones como WhatsApp, Telegram, Facebook, Messenger, Signal, entre otros, son una herramienta para difundir cadenas de mensajes, videos o audios con información manipulada o *fake news* que ayudan a generar pánico o desinformación en las filas enemigas o en la población civil que les sean afectas. Por esta razón, constituyen un factor clave para golpear al enemigo por medio de operaciones de decepción que provoquen su desmovilización del frente de batalla o para asestar golpes fuertes contra su estructura armada por medio de unidades de Fuerzas Especiales.

Ciberataques contra entidades estatales y privadas

Estas acciones van encaminadas a interrumpir las actividades o funciones que cumplen las entidades privadas o públicas de un Estado u organización enemiga. Dado que es difícil identificar y responder a un ataque sin correr el riesgo de dañar o agravar las relaciones con otros Estados o con la contraparte en un conflicto (Silva, 2021), la respuesta apropiada de las autoridades correspondientes puede

ser deteriorar la credibilidad o la funcionalidad de las entidades ante su población civil para generar caos e incertidumbre.

Además, estas acciones sirven para robar información sensible que pueda brindar una ventaja estratégica importante sobre el adversario. Este es el caso del ciberespionaje económico, que puede ahorrar costos de inversión en investigación y desarrollo para un país si se apropia de los avances tecnológicos o la propiedad intelectual de productos de otras empresas o Estados para beneficio propio, como lo ha hecho China en los últimos años contra empresas occidentales.

Respaldo político a la oposición del gobierno adversario

Este método es utilizado por agencias de inteligencia estatales con la aprobación de los gobiernos para fracturar y perturbar el entorno político del adversario y, de este modo, debilitar su proceso de toma de decisiones. Uno de los casos domésticos más famosos fue el de Estados Unidos en 1901, cuando instigó una revuelta armada en los territorios colombianos del actual Panamá para favorecer su independencia y asegurar la construcción del Canal y el control de su área adyacente (Silva, 2021).

Este respaldo incluye aportar una ayuda financiera y los suministros necesarios para que la actividad política opositora sea exitosa, para lo cual es importante saber navegar en la zona gris de confrontación jugando con la ambigüedad de la situación. Por ende, es necesario no dejar huellas o pistas, como transacciones electrónicas o reuniones de la oposición política con agentes o enviados propios, de tal manera que se impida a las agencias de inteligencia o contrainteligencia enemigas obtener pruebas de este respaldo, lo cual reduce la posibilidad de escalar a un conflicto diplomático mayor.

Aquí vale la pena mencionar el caso de Viktor Medvedchuk, un político ucraniano del partido opositor prorruso Plataforma por la Vida, quien es el padrino de una de las hijas de Putin y fue apoyado activamente por la agencia de inteligencia rusa FSB para que creara las condiciones políticas para que Rusia invadiera a Ucrania en febrero del 2022. Mientras algunos analistas lo presentaban como el futuro enlace entre Rusia y una Ucrania derrotada y subyugada al Kremlin, y en Kiev lo llamaban “el príncipe de las tinieblas”, apodo que indicaba su tendencia a moverse en las sombras (Goncharenko, 2022), las agencias de inteligencia ucranianas le seguían los pasos por su evidente apoyo al Kremlin. Después de la fallida toma a Kiev por parte del ejército ruso, se escondió e intentó escapar hacia Rusia, pero fue capturado por los servicios de inteligencia ucranianos en abril del mismo año.

Es decir, solo el conductor estratégico político puede asumir el riesgo de apoyar una oposición política del adversario, pero debe hacerlo después de que haya analizado las consecuencias y, en lo posible, de forma tácita para que pueda avanzar en el cumplimiento de sus objetivos.

Acciones de inteligencia agresivas

Las actividades de inteligencia sobre el enemigo en un conflicto en zona gris se deben hacer de forma agresiva y constante para infiltrar sus servicios secretos de inteligencia, obtener información militar ultrasecreta de sus fuerzas militares o efectuar acciones violentas por medio de agentes reclutados para atacar las instituciones o personas que sean una amenaza para los intereses.

Como ejemplo se puede presentar el caso de las agencias de inteligencia rusas, las cuales efectuaron actividades agresivas de inteligencia en Colombia brindando apoyo el paro nacional en el año 2021. Así lo comprobó el *dossier* de la Central Intelligence Agency (CIA), que prueba el nexo de Rusia con los disturbios en Bogotá mediante su inyección de capital a grupos que estuvieron detrás de los desmanes y los destrozos en las protestas que acontecieron en todo el país, incluso en el año 2019 (*El Tiempo*, 2022). Esto indica que no importa la distancia geográfica que exista con el país objetivo para actuar en un conflicto en zona gris y mantener los intereses. En este caso, se trató de afectar la gobernabilidad del presidente de Colombia, fortalecer la oposición y generar un mejor panorama político al régimen venezolano, que en últimas es el principal aliado de Rusia en la región, junto con Nicaragua y Cuba.

Hechos consumados

Estos implican desafiar la disuasión del actor contrario, al que se busca provocar para forzarlo a que se sobreactúe, principalmente, de forma violenta, de manera que pierda legitimidad interna y externa para dejarlo en una posición forzada. Los referéndums o las declaraciones de independencia constituyen un buen ejemplo (Silva, 2021). Para que el hecho consumado funcione, la ganancia que se vaya a obtener debe ser limitada, de modo que la víctima prefiera dejar pasar estas acciones en lugar de iniciar una escalada que pueda iniciar una guerra armada.

Los hechos consumados son una estrategia común a la hora de ocupar territorios disputados entre dos o más Estados (Jordán, 2018). Por ejemplo, en la anexión de la península de Crimea, la Federación de Rusia utilizó una operación de engaño, ocupó con personal militar y agentes de inteligencia los centros de poder

de la región y desterró a las autoridades ucranianas. De esta manera, con un mínimo de fuerza obtuvo una ganancia territorial importante, lo que generó un hecho consumado que no pudo ser revertido por Ucrania ni la OTAN, ya que hubiera generado una escalada del conflicto con consecuencias graves para todos.

Guerras por delegación o (*proxy wars*)

También llamadas *guerras subsidiarias*, se producen cuando dos o más países utilizan a terceros como sustitutos y así evitar una confrontación de forma directa. Un caso reciente se presentó con el comienzo de la Guerra Fría, cuando la amenaza nuclear agitaba el espectro de una destrucción mutua asegurada, de manera que el recurso a los actores “delegados” comenzó a generalizarse entre las grandes potencias: la Unión Soviética, China y los Estados Unidos (Pontijas, 2020). Por ende, un Estado organizaba o apoyaba a otro Estado, ejército privado o bando en conflicto, brindándole armas, capacitación, entrenamiento militar, financiamiento y asesores, con el fin de que lucharan contra su enemigo sin emplear las fuerzas militares propias.

En la actualidad muchos países utilizan la guerra por delegación para mantener sus intereses, como Estados Unidos, Rusia, Reino Unido, Irán, Turquía, Arabia Saudí, China, Pakistán, entre otros. También lo utilizan actores no estatales, como grandes corporaciones y empresas, grupos terroristas, carteles de la droga, etc. (Pontijas, 2020), con la intención de desgastar las capacidades militares del enemigo en un conflicto armado y así erosionar o desmantelar sus capacidades militares por la confrontación bélica que está desarrollando contra su adversario.

En esta parte de la guerra en zona gris, un conflicto por delegación o *proxy wars* es aquel en el cual el enemigo puede tener claro las intenciones de su adversario y los objetivos que busca. Se trata de un método de guerra híbrida, casi de confrontación directa y que, dependiendo de las armas y los métodos de guerra que se utilicen, podría escalar a una guerra total. Esta es la situación que podría ocurrir en el conflicto entre Rusia y Ucrania, los cuales se encuentran inmersos en una guerra de carácter convencional directa, donde la OTAN, en cabeza de los Estados Unidos, ha enviado armas pesadas y apoyo económico importante para mejorar las capacidades de combate de las fuerzas militares ucranianas.

Esta estrategia ha servido para propinar golpes importantes contra el ejército ruso, de manera que el Kremlin tuvo que cambiar la estrategia y los objetivos que se había propuesto cuando inició sus acciones. Es decir, en lugar de ocupar Kiev y colocar un gobierno prorruso, como se había propuesto, su objetivo se transformó

en lograr el control del oriente del país, la región del Donbas, y arrebatarle la costa del mar negro a Ucrania.

Esta situación podría generar una peligrosa escalada bélica, pues Rusia podría interpretar el apoyo que la OTAN brinda a Ucrania como un acto beligerante, de manera que podría efectuar ataques contra Polonia o los países bálticos en una confrontación directa contra el poder de la organización, que es muy superior al poder militar ruso. Como evidencia este caso, que podría escalar a un conflicto nuclear, en una guerra por delegación se busca crear un conflicto directo con el adversario para debilitar sus capacidades militares y denegarle victorias en el campo de batalla, de tal manera que se logre erosionar su posición en una eventual negociación y preservar así los intereses y objetivos políticos que se plantearon.

Coerción económica

Son las medidas comerciales y financieras fuertes que se aplican contra Estados que se consideren hostiles o que estén interfiriendo en los intereses nacionales. Tienen el objetivo de golpear su capacidad de intercambio comercial internacional y el poder adquisitivo local de su población. Se debe resaltar que en este escenario tiene un papel importante el apoyo a las huelgas nacionales, sectoriales, individuales o coordinadas, entre otras acciones para ejercer una coerción política que refuerce la presión política (Silva, 2021). Estas medidas o sanciones económicas deben ser lo suficientemente fuertes como para que la presión que generan contra el gobierno adversario haga cambiar su posición política en un sentido favorable a los intereses del Estado que realiza las acciones.

Este es el caso de Venezuela, a la que Estados Unidos ha impuesto varias medidas de carácter económico y político para diezmar el poder del régimen, por ejemplo mediante sanciones económicas y el no reconocimiento de su presidencia. Aunque estas acciones han sido poco productivas, el gobierno de Maduro se ha visto forzado a hacer pequeñas concesiones políticas y a efectuar giros en materia económica para mantener el control del país. Específicamente, a través de un proceso de liberalización económica desordenada, ha intentado dar un respiro a la economía para beneficiar a sus élites y a grupos con acceso a divisas, con lo cual ha logrado minimizar las tensiones sociales. Esta transformación desordenada, en vez de debilitar a Maduro, le ha permitido consolidarse en el poder (Jiménez, 2022).

De igual manera, las sanciones contra países como Rusia, por su anexión ilegal de la península de Crimea en 2014, o a Irán en 2018, por su programa nuclear, no han sido efectivas porque estos países encontraron formas de compensar las

presiones externas sin renunciar a sus logros y objetivos. Además, sus medios de comunicación han usado estas sanciones como propaganda para denunciar una agresión a gran escala de Occidente que busca arrodillar al gobierno y la nación a sus caprichos. Estos hechos evidencian que, en un escenario de zona gris, la coerción económica se debe utilizar junto con otros métodos para lograr alguna ganancia estratégica sobre el enemigo.

Sliced salami tactics

Los orígenes del término, que en español se traduciría como “tácticas de corte salami”, se remontan por lo menos hasta finales de la década de 1940, cuando el líder comunista húngaro Mátyás Rákosi afirmó que había logrado derrotar a sus rivales internos incitándolos a abandonar segmentos cada vez más grandes de su propio partido, “cortándolos como rebanadas de salami” (Pusztai & Inántsyt-Pap, 2016). También llamado *obtención de ganancias graduales*, este mecanismo de guerra en zona gris se refiere al compendio o suma de varias acciones de bajo perfil que proporcionan ganancias graduales y que, a la vez, dificultan una reacción severa del adversario (Mazarr, 2015), pues, consideradas individualmente, no justifican su empleo de la fuerza. De esta manera es posible obtener una ventana de discusión o arreglo diplomático para buscar una solución sensata y evitar que el conflicto escale o se decante en una guerra.

Por lo tanto, las *sliced salami tactics* se generan cuando se han realizado varios hechos consumados para erosionar la posición del adversario y que han fortalecido nuestro poder de disuasión y posición en una posible negociación. De esta manera se habrá impedido que el enemigo reaccione, ya que su credibilidad estaría degradada en el momento en que decida actuar, lo cual agravaría su situación. Por ejemplo, Rusia ha efectuado tácticas salami de manera constante durante los últimos veinte años contra sus vecinos regionales, no solo al separar Abjasia y Osetia del Sur de Georgia, y a Crimea de Ucrania, sino también expandiendo sutilmente las vallas fronterizas en Georgia, realizando provocativos vuelos militares sobre Europa del Este y avanzando para controlar los recursos naturales del Ártico (Maass, 2022).

Finalmente, cabe señalar que las tácticas salami y los hechos consumados son exitosos si es posible controlar la ejecución de la escalada y se cuenta con las capacidades militares suficientes para imponerse en el nivel superior de conflicto.

Disuasión militar

Esta herramienta se puede considerar como la última medida disuasoria que se debe adoptar después de haber agotado las demás opciones disponibles, ya que su objetivo es efectuar acciones militares que logren un impacto psicológico en el enemigo. Para esto se demuestra que se cuenta con un poderío militar superior, de tal manera que genere temor al adversario en caso de querer escalar la confrontación o guerra en zona gris.

Como dice Jordán (2014), la disuasión es un proceso que consiste en influir en un actor mediante amenaza, tácita o explícita, con el fin de que no lleve a cabo una determinada acción. La disuasión se puede ejercer antes de que comience un conflicto, con el fin de evitarlo, pero también una vez que han estallado las hostilidades, con el propósito de limitar su alcance geográfico o el nivel de intensidad del enfrentamiento (Jordán, 2014). Por ello se debe evaluar de forma objetiva y profesional el coste/beneficio que podría traer esta acción al aplicarla.

Por otra parte, debe existir un conocimiento profundo de las capacidades militares del enemigo, sea estatal o no estatal, para poder diseñar estrategias de disuasión militar que eviten una escalada hacia una confrontación directa, la cual podría ocurrir por la falta de información sobre los protocolos de respuesta enemiga. Es decir, es fundamental tener claras la doctrina y las capacidades militares que tiene el adversario para contestar el ataque.

Finalmente, para concluir esta exposición, en la figura 1 se sintetizan las oportunidades o mecanismos que se pueden emplear en la zona gris.

Figura 1. Mecanismos que se pueden emplear en una zona gris.

ZONA GRIS	ESTRATEGIAS		OPERACIONES DE INTELIGENCIA
AMBIGÜEDAD	IMPACTAN	Operaciones de influencia sobre la opinión pública internacional y del adversario	ESPIONAJE
GRADUALISMO		Coerción económica	SABOTAJE
INTERESES SUSTANCIALES EN JUEGO		Acciones ofensivas de inteligencia	DECEPCIÓN
ESTRATEGIAS MULTIDIMENSIONALES		Guerras por delegación (proxy wars)	PSICOLÓGICAS
		Sliced salami tactics (obtención de ganancias graduales)	INFORMACIÓN
		Ciberataques contra entidades públicas y privadas	NEUTRALIZACIÓN

Fuente: Elaboración propia.

Zona gris en Colombia

Colombia se ha caracterizado en su historia republicana por combatir a grupos ilegales, estructuras de poder foráneas y comunidades locales que buscan tener el control político, social y económico por medios de la coerción militar o armada en las múltiples actividades ilícitas que suceden en el país. Al ser el primer productor de pasta base de coca del mundo, en el país existen múltiples organizaciones criminales que manejan los diferentes eslabones que intervienen en la producción de estupefacientes, como las disidencias de las FARC, el ELN, el Clan del Golfo, el EPL, grupos de delincuencia organizada regional, entre otros.

Asimismo, intervienen actores extranjeros que apoyan directa o indirectamente el tránsito de estupefacientes a cambio de dividendos económicos, como ocurre con el régimen venezolano, que es considerado por la comunidad internacional y por los organismos multilaterales como el principal puente de salida de la droga de Suramérica hacia otros destinos y continentes. Su situación política, económica y social, así como la corrupción, la inseguridad, la impunidad y el deterioro de los cuerpos de seguridad y de las instituciones del Estado han contribuido al incremento tanto del tráfico como del consumo de drogas en el país (Camero, 2017).

Sumado a esto, filtraciones de documentos reservados del 9 de agosto de 2019 del Servicio de Inteligencia Bolivariano (SEBÍN) y del Comando Estratégico Operacional de la Fuerza Armada Nacional Bolivariana (FANB) evidenciaron la presencia de las disidencias de las FARC y de miembros del ELN en territorio venezolano, los cuales contarían con el apoyo del presidente Nicolás Maduro (López, 2020). Este hecho provoca un grave problema de seguridad fronterizo con el vecino país, pues los grupos irregulares planean desde allí acciones armadas contra las Fuerzas Armadas y atentados contra la infraestructura crítica del Estado, con el objetivo de socavar la cohesión social de las comunidades y suplantar la autoridad del Estado. Además de esta grave situación, también se debe agregar el litigio marítimo entre Colombia y Nicaragua en la Corte Internacional de Justicia de La Haya por las fronteras marítimas del mar Caribe.

Este escenario suscita serios retos para la seguridad y la defensa del territorio colombiano, de manera que es necesario estudiar las diferentes estrategias multidimensionales que se podrían aplicar a estos grupos en una confrontación en la zona gris. Para cumplir este objetivo no son suficiente las acciones legítimas del Estado, como las operaciones militares o policiales, dirigidas a neutralizar a los miembros de las diferentes estructuras armadas que delinquen en el territorio

colombiano, sino que la estrategia también se debe direccionar a deslegitimar las acciones de estos grupos armados de cara a la población civil, que los ve como una autoridad legítima en sus territorios.

Por consiguiente, es posible evaluar la conveniencia de utilizar las operaciones de información o psicológicas para impactar a la población fronteriza y, por qué no, dirigirla contra los integrantes de los diferentes grupos armados para erosionar la confianza y la colaboración que puede existir entre estos. De esta manera, las acciones agresivas entre las estructuras podrían escalar al punto de que se instaure un ambiente propicio para la confrontación directa, lo cual afectaría sus componentes armados y la capacidad de recolección de finanzas que perciben de sus rentas ilegales. Todo esto sin poner en peligro la integridad de los miembros de las fuerzas de seguridad del Estado en una posible confrontación armada con dichas estructuras.

Ahora bien, las estructuras armadas están utilizando masivamente los medios de comunicación electrónicos, como los dispositivos móviles inteligentes, entre sus componentes armados y logísticos para coordinar el recaudo de finanzas y material logístico para su funcionamiento. Esta situación abre una ventana de oportunidad para aprovechar dicha debilidad y con ello obtener nuevas capacidades en equipos de guerra electrónica que brinden a las Fuerzas Armadas alcances novedosos, como la ubicación y hackeo de los equipos móviles, además de utilizar los ciberataques para robar datos y efectuar trabajos de judicialización o nuevas Operaciones de Inteligencia con la información recopilada.

Igualmente, dado que cada grupo armado que delinque en el país, dependiendo del área que controla, genera dinámicas propias de articulación y operatividad ilegal, resulta difícil proponer una estrategia general para atacarlas de forma homogénea. En este sentido, es necesario efectuar un estudio juicioso de las características físicas de terreno, población, infraestructura, vías de comunicación, control territorial, economías locales legales e ilegales, cobertura de los medios de información escritos o de televisión, sean regionales o nacionales, conectividad a servicios de internet y telefonía móvil, entre otros aspectos, con el propósito de analizar las posibles estrategias, no solo dirigidas a golpear la capacidad militar de las organizaciones criminales, sino también para atacarlas de forma integral, en especial quitándole el apoyo de la población civil y sus fuentes de financiamiento.

Por ello es fundamental tener claro el objetivo que se espera cumplir en una guerra en zona gris contra las estructuras criminales, ya que no existirá una victoria física para medir el éxito de la estrategia, sino que en este caso se buscaría

debilitar la capacidad estratégica que podrían tener los grupos armados ilegales y su control sobre áreas del territorio colombiano y la población civil que las habita.

Conclusiones

En un conflicto en zona gris es fundamental usar las Operaciones de Inteligencia como medio para cumplir los objetivos establecidos contra un Estado adversario u organización criminal, al tiempo que se busca preservar los intereses nacionales, como sea que los considere el tomador de decisiones estratégico. Con este propósito, se pueden emplear las operaciones de espionaje, sabotaje, decepción, psicológicas, neutralización o de información, con las cuales es posible impactar la zona gris y obtener ganancias estratégicas importantes sin necesidad de una confrontación armada directa.

Asimismo, existen varios retos en la zona gris, ya que su ambigüedad, intereses en juego y gradualismo hacen que se exploren diversas estrategias multidimensionales, las cuales se concretan con un estudio juicioso y completo del ambiente operacional de la amenaza. En el caso de Colombia, el país tiene problemas de seguridad fronteriza con Venezuela y un diferendo limítrofe con Nicaragua, así como un problema de seguridad interna, pues coexisten múltiples grupos armados que delinquen de diferentes formas. Por estas razones, se deben aplicar estrategias que ataquen su legitimidad como autoridad en las áreas donde operan, degradar el apoyo social que pueda existir en sus áreas de injerencia de manera diferencial y crear conflictos entre sus integrantes para afectar el mando y el control de estas estructuras. Además, es necesario atacar la zona gris con Venezuela y Nicaragua para fortalecer la posición estratégica de Colombia frente a los intereses que ellos buscan en nuestra nación.

Por último, se debe tener claro que la guerra en la zona gris es un conflicto entre las sombras, lo cual borra los límites que podrían existir entre paz y guerra entre naciones u organizaciones involucradas. Además, esta escala a un conflicto permanente o de larga duración que se libra de forma ambigua, por lo que en este espectro no se puede medir la victoria de forma física, sino las ganancias estratégicas que se logran sacar en procura de cumplir los objetivos para salvaguardar los intereses del Estado.

Referencias

- Andrade Rojas, W., Martínez Benavides, J. F., & Pineda Bello, J. C. (2011). *Las operaciones de información en las guerras de información* [Tesis de pregrado, Universidad Piloto de Colombia]. Repositorio UNIPILOTO. <https://tinyurl.com/3f7vpwer>
- Aznar, F. (2015, 25 de noviembre). *Las generaciones de guerras: Guerras de primera generación (I)* [Documento de Análisis, n.º 54]. Instituto Español de Estudios Estratégicos. <https://tinyurl.com/5yca9se5>
- Baqués, J. (2017). *Hacia una definición del concepto Gray Zone (GZ)* [Documento de Investigación, n.º 2]. Instituto Español de Estudios Estratégicos. <https://tinyurl.com/56aeyjde>
- Bolaños, L. F. L. (2018). El día que cambió la historia del arma nacional de Inteligencia. *Perspectivas en Inteligencia*, 10(19), 43-55. <https://doi.org/10.47961/2145194X.50>
- Camero, M. (2017). *El tráfico de drogas ilícitas en Venezuela*. Observatorio de Delito Organizado; Asociación Civil Paz Activa.
- Correa Martínez, S. L. (2017). *La estrategia antiterrorismo de los EE. UU. en Medio Oriente a partir de los atentados del 11S: Aproximaciones desde el mito político del excepcionalísimo norteamericano* [Tesis de pregrado, Pontificia Universidad Javeriana]. Repositorio PUJ. <https://tinyurl.com/4wf8f7dm>
- Cuneo, P. (2019). *Complejidad y multipolaridad en el Sahel: Nuevas dinámicas relacionales y de intervención en el marco de las relaciones internacionales* [Tesis de doctorado, Universidad Pontificia Comillas]. Repositorio Comillas. <https://tinyurl.com/ykknvmpy>
- Del Rey, V., & Canales Torres, C. (2012). *Blitzkrieg: La victoria alemana en la guerra relámpago* (vol. 1). EDAF.
- El Tiempo*. (2022, 26 de marzo). El dossier de la CIA que prueba nexo entre rusos y disturbios en Bogotá. <https://tinyurl.com/hr7yjwcn>
- Gamboa, J. B. S. (2016). Ideas fundamentales sobre inteligencia. En *Inteligencia: Un enfoque integral* (pp. 13-40). Instituto Español de Estudios Estratégicos.
- Goncharenko, R. (2022, 14 de abril). Viktor Medvedchuk, el hombre de Putin en Ucrania. DW. <https://tinyurl.com/2kbh9afu>
- Hoffman, F. (2007). Conflict in the 21st Century: The rise of hybrid wars. Potomac Institute for Police Studies. <https://tinyurl.com/dyc5rmnv>
- Hoffman, F. (2009). Hybrid warfare and challenges. *Joint Force Quarterly*, 52(1), 34-39. <https://tinyurl.com/42ne9y2d>
- Jiménez, M. (2022). *El difícil camino hacia una democratización en Venezuela* [Documentos de Trabajo, n.º 61]. Fundación Carolina; Agenda 2030; Cooperación Española. <https://tinyurl.com/yc4f632w>
- Jordán, J. (2014, 18 de junio). Gestión de la incertidumbre en las relaciones internacionales: Dilema de seguridad, disuasión y diplomacia coercitiva. <https://tinyurl.com/4aw74fx9>

- Jordán, J. (2018). El conflicto internacional en la zona gris: Una propuesta teórica desde la perspectiva del realismo ofensivo. *Revista Española de Ciencia Política*, (48), 129-151. <https://tinyurl.com/3j5h2j39>
- Llop Meseguer, S., Martínez Enríquez, L., & Valeriano-Ferrer Gonzales, F. (2013). *Apuntes de inteligencia básica*. División de Publicaciones de la Escuela Superior e Guerra Naval. <https://tinyurl.com/4anuvwjy>
- López, C. (2020). Agencia, actores, escenarios: La tensa calma de la zona gris sudamericana. *Revista de Pensamiento Estratégico y Seguridad CISDE*, 5(2), 25-39. <https://tinyurl.com/vybftfy>
- Maass, R. W. (2022). Salami tactics: Faits accomplis and international expansion in the shadow of major war. *Texas National Security Review*, 5(1), 33-54. <https://tinyurl.com/29bc2jaa>
- Mack, A. (1975). Why big nations lose small wars: The politics of asymmetric conflict. *World Politics*, 27(2), 175-200. <https://doi.org/10.2307/2009880>
- Mazarr, M. J. (2015, 22 de diciembre). Struggle in the gray zone and world order. *War on the Rocks*. <https://tinyurl.com/5cakh86z>
- Méndez L. A., Gaitán Vanegas, S., & Fuquen, V. P. (2019). Los dominios de la guerra: Una aproximación al nuevo escenario de la Covid-19. *Estudios en Seguridad y Defensa*, 14(28), 237-257. <https://doi.org/10.25062/1900-8325.282>
- Muñoz Ciro, J. S. (2018). *Causas, proyecto político y medios del Estado Islámico* [Tesis de maestría, Universidad de Antioquia]. Repositorio UDEA. <https://tinyurl.com/5n8uxuvs>
- Pontijas, J. L. C. (2020). Tendencias en la guerra por delegación (proxy warfare). *Boletín IEEE*, (18), 85-96. <https://tinyurl.com/4ytzr357>
- Pusztai, G., & Inántszy-Pap, Á. (2016). An underground church-run school during the communist rule in Hungary (1948-1990). *Historia y Memoria de la Educación*, (4), 177-213. <https://doi.org/10.5944/hme.4.2016.15734>
- Quiñónez, R. I. G. (2012). *Curso básico de inteligencia*. S. p. i.
- Raggio, M. L. (2019). El conflicto en las sombras: Aspectos generales y elementos jurídicos de las operaciones en la zona gris. *Cuadernos de Estrategia*, (201), 17-56. <https://tinyurl.com/2yfnn3x>
- Sainz de la Peña, J. A. S. (1991). Estudio de "Inteligencia operacional". *Cuadernos de Estrategia*, (31), 15-37. <https://tinyurl.com/426wst5v>
- Schachtner, A. J. (2018). *Military intelligence in the gray zone: The strategic role of intelligence in unconventional warfare* [Tesis de maestría, US Army Command and General Staff College]. Repositorio DTIC. <https://tinyurl.com/9ccwwew8>
- Silva, J. S. (2021). La zona gris, un desafío para la conducción política y estratégica. *Cuaderno de Trabajo*, (6), 1-19. <https://tinyurl.com/593hxm3>
- Swenson, R. G., & Sancho, C. (Eds.). (2015). *Gestión de inteligencia en las Américas*. National Intelligence University. <https://tinyurl.com/y5uxkp2r>

Waltz, K. (2010). *Theory of international politics*. Waveland Press Inc.

Zavala, O. (2018). *Los cárteles no existen: Narcotráfico y cultura en México*. Malpaso Ediciones SL.