45

Ejército de Chile
Academia de Guerra

Cuaderno de Difusión Pensamiento de Estado Mayor

Noviembre
2021

ISSN 0717-4187

CONTENIDOS

ARTÍCULOS:

PRESENTACIÓN

La Academia de Guerra del Ejército (ACAGUE), en su rol de institución de Educación Superior, desarrolla docencia de pregrado y postgrado, investigación, y vinculación con el medio con el propósito principal de formar Oficiales de Estado Mayor y contribuir a la comunidad educativa institucional y extrainstitucional.

Como es tradición dentro de la investigación académica que se realiza en la Academia de Guerra, el Cuaderno de Difusión del Pensamiento de Estado Mayor, recoge los resultados de investigaciones realizadas por los alumnos en el ámbito de las Ciencias Militares. El presente número recopila artículos escritos por alumnos del Curso Regular de Estado Mayor (CREM) que imparte la Academia de Guerra, así como también del Magíster en Historia Militar y Pensamiento Estratégico, y profesores auxiliares.

En esta oportunidad, el Cuaderno de Difusión aborda cuatro áreas de investigación: Estrategia, Historia Militar, Conducción del Combate y Ciberguerra.

En el área de la Estrategia los alumnos del tercer año del CREM, Mayor Sebastián Jara Castillo, Mayor Marcos Alarcón Vásquez, Mayor Javier Macías Araya y Mayor Carlos Thollander Jeria, presentan el artículo titulado La Guerra del Líbano del 2006: una interpretación desde la Gran Estrategia. A través de un análisis comparativo entre los beligerantes, e incluyendo los factores diplomático, información, militar y económico (DIME), el artículo sostiene que a pesar del importante esfuerzo y desgaste militar, Israel logró conseguir el objetivo de fortalecer la seguridad de su Estado, sin afectar significativamente su desarrollo económico.

En el área de Historia Militar, Carlos Stange Pooley, abogado y egresado del Magíster de Historia Militar y Pensamiento Estratégico, realiza un análisis histórico a la batalla decisiva del Frente Oriental, la Operación Ciudadela en

Kursk (1943). A través de una acuciosa confrontación de fuentes históricas primarias y secundarias, el autor discute la relevancia de dicha batalla y logra determinar los efectos que ésta tuvo para el resultado de la Guerra en el Frente Oriental y dilucidar si es apropiado catalogarla como decisiva.

En el área de Conducción del Combate, el Mayor Gerardo Hermosilla Acevedo, profesor auxiliar de la Academia de Guerra, reflexiona sobre la validez de aplicar los Principios de la Guerra a la Contrainsurgencia. En este artículo el autor concluye que, a diferencia de lo que se conoce como guerra regular, en la guerra irregular la aplicación de dichos principios es mucho más compleja, principalmente, debido a las condiciones donde ésta se desarrolla y la disputa que se produce por el apoyo de la población civil y la exposición a los medios de comunicación social.

En el área de la Ciberguerra, el alumno del tercer año del CREM, Mayor Juan Pablo Nieny Hodar, reflexiona sobre posibles efectos e impacto de la tecnología 5G en el ámbito de la Ciberseguridad. En este trabajo, se presentan las ventajas en el uso de esta tecnología, pero también se dan a conocer distintos desafíos a considerar una vez implementada.

Por su parte, el Mayor Rodrigo Kinast Werner, profesor auxiliar de la Academia de Guerra, analiza el concepto de disuasión y el uso de la legítima defensa en el ciberespacio. Un tema contingente y atingente que contribuye a la visualización del desempeño de las capacidades militares en el ciberespacio. En el artículo, el autor revisa la aplicabilidad del concepto de disuasión tradicional y sus elementos constitutivos respecto a esta relevante dimensión. Asimismo, ejemplifica los aspectos teóricos tratados e identifica desafíos utilizando tres casos de estudio: los ataques ocurridos en Estonia, en la Guerra de Osetia del Sur y en la planta nuclear de Natanz en Irán.

Finalmente, considerando el contexto especial y las tareas propias a las cuales se ha visto enfrentado tanto el país como la Institución y sus integrantes,

producto de la emergencia sanitaria vigente, expreso mi agradecimiento a los profesores auxiliares y alumnos en la elaboración de esta edición del Cuaderno de Difusión del Pensamiento de Estado Mayor, quienes a través de un importante esfuerzo individual sometieron a revisión y crítica los resultados de sus investigaciones y estudios, con el fin de perfeccionar sus habilidades académicas para transmitir y compartir sus hallazgos.

Pongo a disposición de nuestros alumnos y docentes, así como de la comunidad académica en general, el presente número del Cuaderno de Difusión que, sin duda, constituye un aporte para el estudio de las Ciencias Militares.

ÁLVARO SALAZAR JARA
Coronel
Director Academia de Guerra

Artículos

LA GUERRA DEL LÍBANO DEL 2006, UNA INTERPRETACIÓN DESDE LA GRAN ESTRATEGIA

The 2006 Lebanon War, an interpretation from the Great Strategic perspective

MAY. Sebastián Jara Castillo*

MAY. Marcos Alarcón Vásquez*

MAY. Javier Macías Araya*

MAY. Carlos Thollander Jeria*

Resumen: La guerra del Líbano 2006 fue un conflicto que enfrentó a Israel con el grupo armado Hezbollah durante 33 días. Este conflicto es interesante de analizar, puesto que Hezbollah empleó nuevas formas para enfrentarse a la potencia militar. Asimismo, en este conflicto Israel, por primera vez, no obtuvo una victoria militar categórica, generando una serie de dudas sobre las reales capacidades de su fuerza para asegurar la supervivencia de la nación en el futuro.

El presente artículo sostiene que, a pesar del gran esfuerzo y desgaste militar, Israel logró conseguir el objetivo de fortalecer la seguridad del Estado, sin comprometer significativamente su desarrollo económico, debido a que armonizó los instrumentos claves del poder nacional robusteciendo su Gran Estrategia.

Palabras claves: poder nacional, armonía, supervivencia, objetivos nacionales

* Oficial del Arma de Infantería. Actualmente es alumno del Tercer año del Curso regular de Estado Mayor en la Academia de Guerra del Ejército de Chile. ✉sebastian.jara@acague.cl

* Oficial del Arma de Infantería. Actualmente es alumno del Tercer año del Curso Regular de Estado Mayor en la Academia de Guerra del Ejército de Chile. ✉marcos.alarcon@acague.cl

* Oficial del Arma de Telecomunicaciones. Magister en Historia Militar y Pensamiento Estratégico. Actualmente es alumno del Tercer año del Curso Regular de Estado Mayor en la Academia de Guerra del Ejército de Chile. ✉javier.macias@acague.cl

* Mayor Carlos Thollander Jeria. Oficial del Arma de Infantería. Actualmente es alumno del Tercer año del Curso Regular de Estado Mayor en la Academia de Guerra del Ejército de Chile. ✉carlos.thollander@acague.cl

Abstract: The 2006 Lebanon War was a conflict that faced Israel against the armed group Hezbollah during 33 days. This conflict is interesting to analyze, since Hezbollah employed new manners to confront the Israel military power. Likewise, this confrontation is the first time in which Israel did not obtain a categorical military victory. This implied several doubts about the real capabilities of its force to ensure the survival of the nation in the future.

This article argues that, despite the defeat, Israel managed to achieve the objective of strengthening the security of the State, without significantly compromising its economic development, because it harmonized the key instruments of national power, strengthening its Grand Strategy.

Key words: national power, harmony, survival, national objectives

INTRODUCCIÓN

El 12 de julio del año 2006, una patrulla militar israelí fue atacada por el grupo armado Hezbollah en la frontera con el Líbano, dejando un saldo de ocho soldados muertos y dos secuestrados.

La intención del grupo era intercambiar estos soldados por los prisioneros que Israel tenía cautivos. Desde aquel día y hasta el 14 de agosto del mismo año, se desarrolló un conflicto bélico donde un Estado combatía a un actor no estatal, cuyas nuevas formas de hacer la guerra daría pie a un amplio desarrollo teórico sobre los conflictos bélicos en el siglo XXI.

La guerra se caracterizó por acercar el conflicto a la población civil, con el objetivo de restar valor relativo a la fuerza militar como mecanismo eficiente para la resolución de conflictos. Inmediatamente después de la firma del acuerdo de paz, diversos analistas coinciden en sostener que Hezbollah, un grupo insurgente, tuvo la capacidad de enfrentarse a una potencia militar, como lo es Israel y no capitular en el intento. Sin embargo, al analizar las diversas dimensiones del enfrentamiento, la afirmación de que Israel fue el real vencedor debe considerarse plausible. El dar cumplimiento a su permanente gran objetivo nacional de supervivencia frente a la amenaza directa de sus vecinos y otros estados de la región y haber aumentado el nivel de seguridad de

sus fronteras, permiten inferir que el Estado de Israel obtuvo importantes ventajas a partir del término de las hostilidades.

El presente artículo tiene por finalidad demostrar que tras el conflicto, Israel logró conseguir el objetivo de fortalecer la seguridad del Estado, sin afectar significativamente su desarrollo económico. En este sentido, aunó instrumentos claves del poder nacional para robustecer su Gran Estrategia[1].

Para ello, se realiza un análisis a los cuatro elementos que representan la articulación del poder nacional, a saber: el poder diplomático, el poder de la información, el poder militar y el poder económico. Estos elementos fueron empleados por Israel armónicamente en la búsqueda de sus objetivos nacionales, incrementado la seguridad nacional y logrando disuadir a sus adversarios de futuros ataques en su frontera norte. Lo anterior, tiene asidero en la teoría planteada por Edward Luttwak (2005) que indica qué para que un Estado sea exitoso debe articular en forma armónica todos los instrumentos del poder nacional, tanto en sus dimensiones verticales como en sus dimensiones horizontales permitiendo una concordancia en la aplicación del poder nacional, aun aceptando derrotas militares menores.

A modo de hipótesis planteamos que en la dimensión diplomática que Israel empleó exitosamente ante las Naciones Unidas, potencias de Occidente y foros de influencia global ante la adversidad en la región, logró configurar un escenario favorable como resultado del conflicto, lo que le permitió aumentar la seguridad del país en el contexto regional. En la dimensión de la información, logró influir con su discurso en el Consejo de Seguridad de las Naciones Unidas y recuperar la cohesión del pueblo de Israel cuestionado al término de las hostilidades, alterando las percepciones de los países del Medio Oriente al término del conflicto. En la dimensión militar, Israel recuperó la capacidad disuasiva logrando una paz negativa en su frontera norte. Finalmente, en la dimensión económica, equilibró el esfuerzo bélico con el resto de los instrumentos del poder nacional, es decir, diseñó una intervención militar a bajo costo con una participación internacional razonable luego de la resolución de la ONU.

[1] Según Liddell Hart (1967), la Gran Estrategia coordina y dirige todos los recursos de una nación, o de un grupo de naciones, hacia la consecución del objeto político de la guerra.

LA DIPLOMACIA PAVIMENTA EL CAMINO A LA VICTORIA

La diplomacia es uno de los instrumentos del poder nacional a través del cual los gobiernos buscan alcanzar sus intereses nacionales.

Su éxito depende de la coordinación y vinculación con otros instrumentos tales como el militar, económico y la información. En este sentido, la responsabilidad de su ejercicio recae en la estructura que cada Estado haya establecido para la difusión de su política exterior y la relación con otros actores internacionales. En relación con lo anterior, el presente apartado sostiene el argumento que el poder diplomático de Israel fue capaz de persuadir a la comunidad internacional en tres niveles:

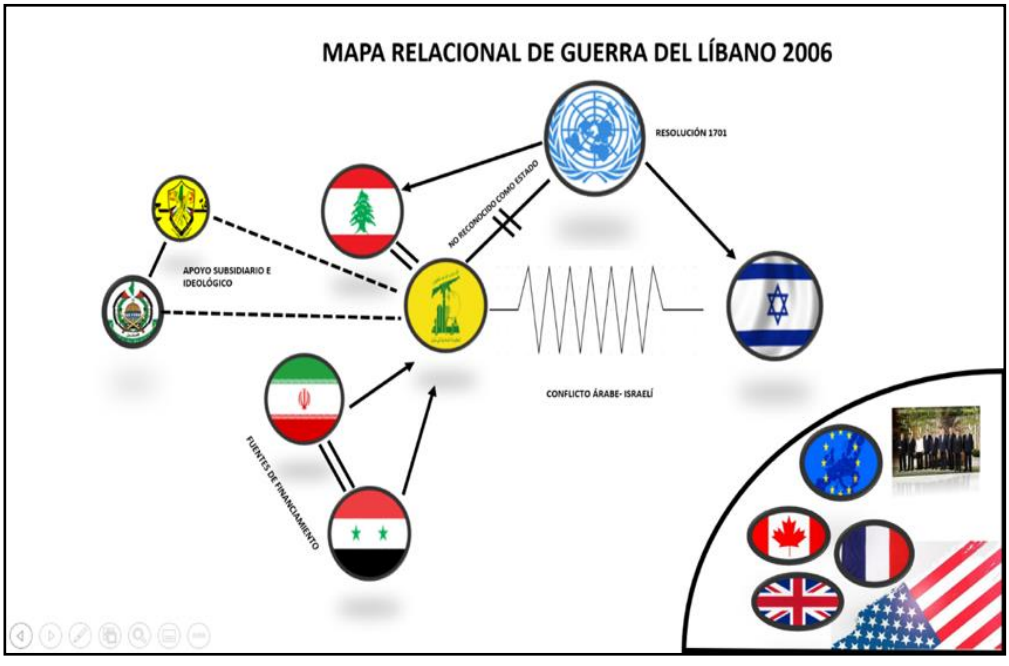
1) Fortaleciendo las relaciones bilaterales con sus aliados estratégicos;

2) Difundiendo su discurso en los foros internacionales más influyentes;

3) Difundiendo la postura israelí en forma explícita y reiterada en el Consejo de Seguridad de las Naciones Unidas.

Figura 1

Relación de actores en el conflicto



Nota. Elaboración propia.

A partir de lo anterior, consiguió un resultado favorable en la resolución Nº1701 del Consejo de Seguridad y posterior firma del cese al fuego, incrementando con esto la seguridad del país en el contexto regional.

Desde el inicio de las hostilidades se evidencia una estrategia por parte de Israel en busca de apoyo internacional en los tres niveles mencionados. De acuerdo con los registros revisados, Israel recibe el respaldo inmediato de sus aliados estratégicos. Así lo demuestran las declaraciones públicas efectuadas por los gobiernos de Estados Unidos y Gran Bretaña quienes adjudican a Hezbollah la responsabilidad en el inicio de las hostilidades, justificando el uso de la fuerza de Israel "en su intento de eliminar la amenaza de Hezbollah en el norte de su territorio" (Consejo de Seguridad 2006).

Por otra parte, Israel acude a dos importantes foros internacionales en busca de difundir su perspectiva del conflicto y conseguir los apoyos necesarios en la Asamblea General de las Naciones Unidas, ocupando las plataformas del G-8 y el Consejo de la Unión Europea para contrapesar la adversidad que presenta en el nivel regional.

En general, las declaraciones publicadas al término de ambos foros coinciden en manifestar su preocupación por el alto número de bajas civiles y en condenar los ataques efectuados por Hezbollah a Israel, los cuales se describen como "un obstáculo que entorpeció los avances en el proceso de paz entre Siria, Líbano e Israel" (Amado, 2006). Por lo tanto, exigen el desarme inmediato de las milicias libanesas y no libanesas en su territorio. En otras palabras, ambos foros reconocen el derecho de legítima defensa de Israel en su frontera norte, además, en ambas instancias se refleja el éxito de la diplomacia de Israel, debido a que se logró instaurar el mensaje que la presencia de Hezbollah, en la frontera sur del país, impedía que el Estado libanés ejerciera el control total de su territorio; por lo que existía el riesgo de un futuro enclave en el Estado musulmán. No obstante, el foro de la Unión Europea adjudica responsabilidades a Israel por los cuantiosos daños provocados a la infraestructura civil a causa de la desproporcionalidad en el empleo de la fuerza

militar, idea que no tendría repercusiones en la resolución elaborada por el Consejo de Seguridad de la ONU.

En el plano de las gestiones diplomáticas frente a las Naciones Unidas, Israel emplea su poder en forma enérgica desde el inicio de las hostilidades. El análisis documental de los discursos emitidos por el Ministerio de Asuntos Exteriores de Israel refleja las reiteradas interacciones que la cancillería tuvo con la ONU a partir del 12 de julio del año 2006. Bajo este contexto, se puede destacar en los discursos pronunciados en cada una de las intervenciones israelitas, la necesidad de posesionar en dicha organización dos potentes ideas centrales. En primer lugar, la idea de que Hezbollah ha provocado una situación de ingobernabilidad en territorio libanés, debido a que el mencionado grupo armado ha tomado el control de la frontera sur impidiendo ejercer al Estado su soberanía. Segundo, que el conflicto en desarrollo entre Israel y Hezbollah debe ser considerado por la ONU como una oportunidad para que la comunidad internacional se integre en una causa justa contra el terrorismo y colabore en restablecer el estado de derecho en su vecino país liberándolo de las ataduras del terrorismo (MFA Israel, 2013).

A la luz de lo anterior, si se confronta la información antes presentada con los diferentes puntos que contiene la Resolución del Consejo de Seguridad de las Naciones Unidas Nº1701, se puede concluir que la estrategia diplomática elaborada por Israel para enfrentar la guerra del Líbano 2006 fue exitosa en su totalidad. Ello quedó demostrado con el apoyo casi unánime de los países integrantes del Consejo de Seguridad de las Naciones Unidas a la postura de legítima defensa propuesta por Israel.

Por otra parte, la Resolución Nº1701 impuso explícitamente al Estado libanés la tarea de tomar el control absoluto de su territorio junto con comprometerse al desarme total de toda fuerza paramilitar libanesa o no libanesa presente en su territorio, que dificultaba el accionar de sus propias Fuerzas Armadas. Junto a lo anterior, se dispuso la presencia de una fuerza de paz de 15.000 hombres para colaborar al control de la frontera entre ambos países (UNSC, 2006); eliminando con este acto las probabilidades de amenaza desde el norte del mundo árabe a territorio de Israel, por

lo tanto, se evidencia la contribución del poder diplomático al aumento de la seguridad de este país.

Finalmente, el éxito de la diplomacia judía se reforzó en el hecho que no existieron sanciones de ningún tipo por parte de la comunidad internacional hacia Israel, a pesar de las graves acusaciones, provenientes del mundo árabe, de provocar daño a la infraestructura civil y violaciones a los derechos humanos, derivadas de la desproporcionalidad en el uso de la fuerza durante los 33 días de hostilidades.

LA INFORMACIÓN COMO INSTRUMENTO DOMINANTE

En los conflictos actuales, la información puede ser usada como un elemento más en la guerra, a través de una maniobra de información y a la vez como un instrumento del poder nacional en sí mismo que contribuye a la gran estrategia. Así también, el incremento de las nuevas tecnologías de la información y comunicaciones (TIC) han tenido una contribución exponencial sobre las técnicas, tácticas y estrategias a emplear sobre el adversario. Por otra parte, como instrumento del poder nacional la dimensión de la información tiene el objetivo de crear realidades favorables para el Estado, contribuyendo a alterar la percepción de los actores involucrados en el conflicto y, también, sobre otros actores, de tal manera de moldear sus conductas obteniendo beneficios que aporten a la gran estrategia del Estado.

En consecuencia, el presente apartado busca argumentar que, en el conflicto del Líbano 2006, Israel logra influir en el Consejo de Seguridad de las Naciones Unidas, recuperar la cohesión del pueblo de Israel cuestionado al término de las hostilidades y, finalmente, modificar la percepción que los países del Medio Oriente tenían de él.

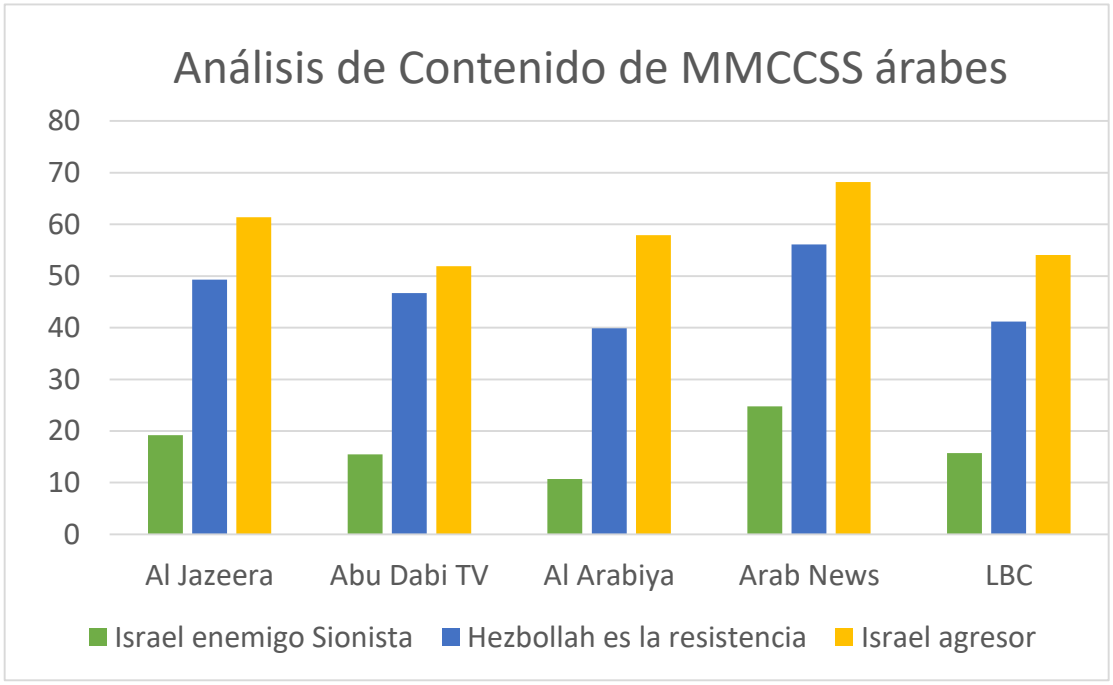
Para comprobar lo anterior, el factor de la “Información” se ha dividido en tres aspectos, siendo estos: 1) El análisis de contenido sobre la guerra del Líbano 2006 en medios de comunicación árabes y Occidentales entre el 2006 y 2010; 2) La fortaleza del discurso y narrativa de los beligerantes frente a Naciones Unidas (ONU) y; 3) El efecto en la modificación en las conductas de los países de Medio Oriente y Estados Unidos.

Conforme al análisis efectuado, la rápida expansión de los medios de comunicación de origen árabe y la profunda penetración de las TIC a nivel global se presentan como los dos principales factores que favorecen la rápida propagación del mensaje de Hezbollah a nivel regional y global.

De acuerdo con un estudio publicado por la Universidad de Harvard (Seib, 2007), la revolución y expansión de las cadenas de comunicaciones que el mundo árabe desarrolló a partir del año 2005 crearon una plataforma robusta de influencia en el mundo islámico. De esta forma, la principal audiencia del conflicto (la región del Medio Oriente) se informaba sobre el conflicto por alrededor de 10 cadenas televisivas que en su conjunto controlaban más de 150 canales de televisión satelital, superando considerablemente la cobertura brindada por cadenas de televisión occidental.

Gráfico 1

Cantidad de menciones hacia Israel en MMCCSS de origen árabe durante el segundo semestre de 2016



Nota. Elaboración propia de acuerdo a los datos obtenidos en publicaciones emitidas por las cadenas Al Jazeera, Abu Dabi TV, Al Arabiya, LBC y Arab News, durante el segundo semestre de 2016.

En este sentido, Hezbollah comprende que las capacidades mencionadas en combinación con un potente mensaje son la clave para dominar el ambiente de la información en la guerra.

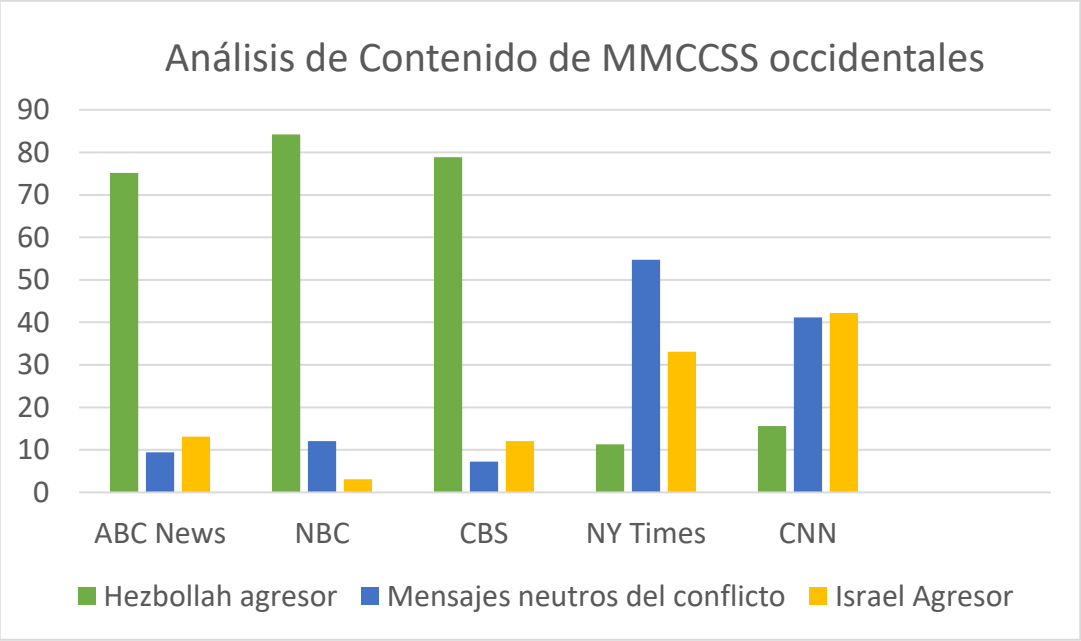
Las publicaciones de Al Jazeera, Abu Dabi TV, Al Arabiya, LBC y Arab News, coinciden en referirse a Hezbollah como “La Resistencia” causando un efecto psicológico en la audiencia en contra del “enemigo sionista”. Además, los registros de tráfico de internet en Medio Oriente, desde los días previos a las hostilidades, dan cuenta de lo determinante que fue esta plataforma para expandir la narrativa islámica, la que permitió posicionar a Israel como “un país agresor” en diferentes sitios web oficiales, foros islámicos, blogs, sitios de distribución, grupos mediáticos y redes sociales. El porcentaje de visitas al interior de Medio Oriente superó el 75% (MFA Israel, 2013).

Por otra parte, el análisis de los principales medios de comunicación occidentales no entrega una tendencia clara en el contenido del mensaje. A saber, solo las cadenas ABC, NBC y CBS mantienen en todo momento la postura de que Hezbollah es el agresor en el conflicto, el resto de los medios fluctúan entre mantener una postura neutral hacia los dos beligerantes y responsabilizar como agresor a Israel en una proporción de 2/3 de sus publicaciones en favor de la neutralidad.

Este aspecto se identificó como el principal obstáculo para la difusión de la narrativa de Israel sobre el conflicto y, por ende, este actor tuvo una limitada capacidad de influir en la opinión pública durante el desarrollo de las hostilidades. Lo anterior se observa en el siguiente gráfico.

Gráfico 2

Cantidad de menciones sobre el conflicto en MMCCSS occidentales, durante el segundo semestre de 2006.



Nota. Elaboración propia de acuerdo a los datos obtenidos de publicaciones emitidas por las cadenas ABC, NBC, CBS, NY Times y CNN durante el segundo semestre de 2006.

En cuanto a la representación frente a la ONU, las capacidades de la estructura diplomática de Israel sumado al respaldo de sus aliados occidentales le permitieron prevalecer con un potente discurso sobre su adversario compensando la falta de influencia en la opinión pública.

Conforme a los archivos históricos de la ONU consultados[2], desde la perspectiva árabe las negociaciones fueron encabezadas por la diplomacia del Estado libanés, instancia donde Hezbollah no tuvo ninguna oportunidad de participación ni de solicitud de demandas a los países de la ONU (MFA Israel, 2013). El Líbano concurre a las negociaciones con tres demandas centrales:

[2] Los archivos históricos revisados corresponden a las cartas emitidas por el Estado Libanes al Consejo de Seguridad de las Naciones Unidas y al Secretario General de la misma organización entre el 30 de julio hasta el 11 de agosto del 2006.

1) Terminar con la violencia;

2) Asegurar la entrada de tropas de la ONU bajo capítulo VI;

3) El compromiso de tomar el control de la totalidad de su territorio para restablecer la unidad nacional (MFA Israel, 2013), aspectos que no estaban alineados con el discurso de Hezbollah al término de la guerra.

Ante tales intereses, la contraparte del Consejo de Seguridad encabezada por Estados Unidos y Francia impone un borrador de la Resolución de la ONU, el que sufrió escasas modificaciones resguardando la postura y los intereses de Israel a causa de la exitosa maniobra diplomática analizada en apartados anteriores. A saber, la resolución Nº1701 impone amplias restricciones al Estado árabe con el objetivo de lograr el desarme definitivo de Hezbollah, favoreciendo los intereses de Israel (UNSC, 2006). Lo anterior, permite inferir el alto grado de influencia ejercido por Israel y sus aliados en la ONU a pesar de no haber obtenido una victoria militar y ser considerado, por parte de la opinión pública en Medio Oriente y a nivel global, como el Estado agresor del conflicto.

Finalmente, Israel consciente de haber perdido el dominio del ambiente de la información durante el período de hostilidades, inicia la articulación de la información en su gran estrategia con la intención de cambiar la percepción de los países de Medio Oriente a su conveniencia, a raíz del resultado del conflicto.

En el ámbito interno, el Estado de Israel modifica el discurso del resultado de la guerra para recuperar la cohesión de su pueblo. De acuerdo a los antecedentes publicados por la comisión investigadora del proceso de toma de decisiones en el conflicto (2007), el gobierno de Israel comienza la articulación de un nuevo discurso hacia la población judía a partir del mes de diciembre del año 2006, el cual transita desde “aceptar una derrota militar frente a Hezbollah” hacia la “pérdida de oportunidad para obtener una victoria” (Jewish Virtual Library, 2008). Asimismo, la estrategia comunicacional para conmemorar el conflicto se centró en destacar algún hecho heroico o actuación individual sobresaliente durante el desarrollo de la guerra, por sobre el contexto general del conflicto. Lo anterior, buscaba recuperar y fortalecer

la voluntad nacional israelí y el apoyo al gobierno central el cual cayó significativamente luego del término de la guerra (Jewish Virtual Library, 2008).

Por otra parte, las conclusiones publicadas en el libro "All Glory is Fleeting" (Glenn, 2012) establecen que, consciente de la información y lecciones entregadas por Israel a fines del año 2006, Estados Unidos aborda la problemática de las nuevas formas de hacer la guerra, lo que da origen al nuevo concepto de "guerra híbrida". A raíz de lo anterior, Estados Unidos incluye a Irán como una de sus principales amenazas en la región debido a su potencialidad en el empleo de fuerzas proxys[3], razón por la cual impuso nuevas sanciones amparadas en la necesidad de limitar el progreso del programa nuclear iraní en el año 2007 (Glenn, 2012).

Israel supo aprovechar el fortalecimiento de Hezbollah alcanzado al término de las hostilidades, apelando a la disputa entre las etnias sunnitas y chiitas en la región. Al hacer una revisión diacrónica del discurso de las autoridades de Israel, éste permite concluir que a partir del año 2008 este reconoce que "las falencias del Ejército en el año 2006 se convirtieron en una fortaleza en el largo plazo" (MFA Israel, 2013), debido a que la permanencia de Hezbollah y el incremento en el liderazgo regional iraní intensificaron la disputa étnica entre las dos facciones del Islam, división que favoreció el desarrollo de conflictos internos en los estados vecinos y disminuyó la probabilidad de Israel para enfrentar un conflicto interestatal.

Como se observa en el análisis de contenido de las publicaciones árabes y occidentales a nivel regional y global, las orientaciones del discurso frente a las Naciones Unidas y el impacto del discurso israelí en las percepciones de los países de Medio Oriente permiten concluir que el ambiente de la información durante el desarrollo de las hostilidades fue desequilibrante para influir en la opinión pública en favor de la causa de Hezbollah. Sin embargo, esta influencia tuvo efectos limitados debido a que Israel logra, con una nueva articulación del ambiente de la información, un correcto empleo de la diplomacia y un coherente uso del poder militar, imponiendo

[3] Un "proxy" es un término que se emplea para hacer referencia a estados intermediarios entre dos potencias, donde la intención del Estado que los emplea es no llegar a un enfrentamiento directo.

sus intereses en las Naciones Unidas, obteniendo el favor en la redacción de la resolución Nº 1701.

Finalmente, se puede comprobar que el cambio en la estrategia comunicacional de Israel luego del término de la guerra influyó en el comportamiento de Estados Unidos en la región y agudizó la disputa entre las etnias sunnitas y chiitas a causa del emergente liderazgo de Irán en el Medio Oriente.

EL PODER MILITAR, OPINIONES DIVERSAS

El poder militar es concebido por el nivel político como un elemento integral del poder nacional, que debe ser empleado teniendo presente la complejidad de los elementos y capacidades que lo componen. La existencia del Ejército, Armada y Fuerza Aérea con capacidades y ámbito de acción diferentes, plantean al conductor estratégico la dificultad de integrar y emplear tales capacidades de la manera más efectiva posible, permitiéndole alcanzar los objetivos planteados, de acuerdo con los lineamientos del nivel político.

Consecuentemente, el presente apartado sostiene el argumento que la articulación del poder militar permitió recuperar la capacidad disuasiva de Israel, entregando una calma relativa en los cinco años posteriores a la guerra, lo que se debe a una efectiva estrategia disuasiva aplicada durante la guerra a Hezbollah y el Líbano.

Israel empleó su fuerza militar con una estrategia caracterizada por:

1) Uso limitado de fuerzas en el conflicto;

2) El desequilibrio en las fuerzas desplegadas entre el Líbano y Hezbollah;

3) La mantención de la tendencia de empleo de la fuerza relacionada a la estrategia de seguridad y defensa;

4) El desarrollo de una tenue maniobra conjunta en el teatro de operaciones.

Para demostrar lo anterior, se realizó un análisis de las fuerzas declaradas por los beligerantes en el conflicto; luego se desarrolló un análisis al comportamiento político

y estratégico en los principales conflictos en los que ha participado. Finalmente, se indagó en las principales acciones que desarrolló Israel como parte del conflicto.

En lo referido al empleo de medios humanos en el esfuerzo bélico, las Fuerzas de Defensa Israelí (IDF), emplearon solo 9.000 hombres (Merom, The Second Lebanon War: Democratic Lessons Imperfectly Applied, 2008), lo que significó un bajo porcentaje de sus fuerzas en el conflicto, considerando la suma total de fuerzas activas: 168.000 hombres en condiciones de entrar en combate (Ejército: 125.000 hombres; Armada: 8.000 efectivos; Fuerza Aérea: 35.000 hombres; Paramilitares: 8.050 efectivos). A lo anterior, se suma una reserva que contaba con un total de 408.000 hombres (Ejército: 380.000; Armada: 3.500; Fuerza Aérea: 24.500) (International Institute for Strategic Studies, 2007, p. 212). Por lo tanto, estos 9.000 hombres representaban solo un 1,8% del total de las fuerzas disponibles. En este sentido, los efectos que generó la decisión del empleo limitado de efectivos son coherentes con el uso del poder diplomático, el poder de la información e incluso el poder económico, permitiendo un equilibrio entre el discurso entregado a la comunidad internacional y las acciones desarrolladas en el conflicto, a través de un empleo armónico de los instrumentos del poder nacional. De esta manera, se estima evitó ser cuestionado por los actores internacionales y logró influenciar en la ONU a través de la Resolución Nº 1701 como se ha señalado en apartados anteriores.

En lo que respecta a las fuerzas del Líbano y Hezbollah, el primero contaba con una fuerza efectiva de 62.0000 hombres entre las Fuerzas Armadas (Ejército: 60.000; Armada: 1.000; Fuerza Aérea: 1.000) y 13.000 paramilitares, mientras que Hezbollah con una fuerza aproximada de 2.000 hombres para el esfuerzo bélico (International Institute for Strategic Studies, 2007).

Lo anterior, permite identificar una desproporción entre las fuerzas de los beligerantes. En consecuencia, a pesar de las nuevas estrategias empleadas por parte de Hezbollah y el Líbano, la IDF logró contenerlas en el momento adecuado, a través de un empleo controlado de su poder militar. El objetivo de esta decisión fue evitar un incremento en la percepción negativa de la opinión pública hacia Israel, y a la vez, suprimir los problemas que hubiera demandado una nueva ocupación del

territorio libanés, como lo fue durante la 1ª Guerra del Líbano (Merom, The Second Lebanon War: Democratic Lessons Imperfectly Applied, 2008).

Desde un punto de vista histórico, el comportamiento de Israel en los conflictos se caracteriza por el permanente espíritu de supervivencia en la región, por lo que su estrategia y doctrina obedecen a una lógica de una rápida ofensiva que permita recuperar la iniciativa y libertad de acción obteniendo espacio y tiempo en el campo de batalla. Para visualizar lo expuesto, es necesario observar la historia de Israel y su comportamiento en conflictos pasados, como lo son: la 1ra Guerra Árabe Israelí (1948-1949), Crisis del Canal de Suez (1956), La Guerra de los Seis Días (1967), La Guerra de Yom Kippur (1973), 1ª Guerra del Líbano (1882-1983), además de los conflictos permanentes y latentes con Hezbollah, Hammas y Al Fatah, donde ha peleado con determinación en cada una de las guerras que han amenazado con vulnerar su supervivencia (Gloffka, 2012), manteniéndose fieles a sus pilares de seguridad nacional: disuasión estratégica, alerta temprana y decisión en el campo de batalla (Henriksen, 2012, p. 111). A la vista de los antecedentes expuestos, el comportamiento de Israel difiere a la tendencia demostrada, lo que finalmente le permite alcanzar objetivos en el nivel de la gran estrategia, permitiéndole una paz duradera en los años posteriores.

Sumado a lo anterior, y referido a su estrategia de seguridad y defensa hasta 1987 las IDF se caracterizaron por seguir los parámetros oficiales de la noción de guerra convencional, que estipulaba tres criterios básicos para evaluar un plan defensivo: disponibilidad de profundidad suficiente para un despliegue escalonado, reservas capaces de realizar un contraataque para restaurar la situación inicial y una distancia adecuada al interior estratégico. En los años posteriores, Israel mantuvo su política de emprender ataques preventivos contra sus enemigos mientras todavía eran demasiado débiles como para resultar amenazadores (Escuela Superior de Guerra Conjunta de las Fuerzas Armadas, 2016). Por lo que, resulta coincidente la estrategia de ataques preventivos de corta duración en la aplicación del poder militar en el conflicto en estudio permitiendo, de esta manera, a pesar de un aparente resultado desfavorable en la guerra, inferir una victoria en el post conflicto. Lo anterior facilitó

que, en los años siguientes, Israel lograra una estabilidad permanente en su frontera norte, disuadiendo a sus adversarios e incrementando el nivel de seguridad del país.

De acuerdo con los registros analizados, la maniobra operacional por parte de Israel fue de una escasa capacidad de integración conjunta en beneficio de los objetivos estratégicos y políticos, ya que a través de la designación de un conductor operacional de la Fuerza Aérea, el General Dan Halutz, se efectuó un marcado esfuerzo en el poder aéreo y una baja participación terrestre. Esto ha llevado al cuestionamiento del empleo del poder militar, lo que se confirma en el informe de la Comisión Winograd, donde se etiquetó al Primer Ministro, el Ministro de Defensa y el Jefe de Estado Mayor de la IDF como incompetentes para manejar la guerra (Henriksen, 2012, p. 117).

Aunque el propio cuestionamiento israelí, permitió fundamentar su mala actuación en esta guerra. Se debe aceptar como plausible la afirmación de que el empleo del poder militar de Israel fue a través de una estrategia limitada, en beneficio de un objetivo nacional superior (supervivencia nacional) por lo que su articulación como parte del poder nacional colaboró en la consecución de objetivos en la gran estrategia.

Finalmente, el empleo del poder militar bajo un concepto de equilibrio y armonía, como parte del poder nacional de Israel, permitió una aplicación coherente y pertinente, efectuando una eficiente coordinación con el poder diplomático, el poder de la información y el poder económico, logrando en su conjunto un efecto de paz negativa que se evidenció en los cinco años posteriores a la guerra.

LA ECONOMÍA SILENCIOSAMENTE GANA LA GUERRA

Sin utilizar las armas los estados pueden verse enfrentados a situaciones de caos y pánico muy similares a la guerra. Aunque la economía es un asunto complejo, es muy difícil desconocer la relación directa que ésta tiene con la seguridad nacional. En cuanto a instrumento del poder nacional, la economía es catalogada como el poder más versátil y flexible para poder influir en el comportamiento de otros actores, por lo que un acabado conocimiento del poder económico de las naciones puede colaborar

significativamente en comprender la forma en que se integrará a la Gran Estrategia del Estado.

Bajo este marco, el siguiente argumento tiene como propósito demostrar que, desde el comienzo del conflicto, el factor económico ha sido un elemento favorable a Israel en comparación a su contraparte libanesa. En este sentido, se puede afirmar que una adecuada articulación del poder nacional israelí le permitió:

1) Solventar de manera eficiente una campaña militar en busca de disminuir los recursos de Hezbollah;

2) Prevalecer como una economía estable y confiable a nivel global;

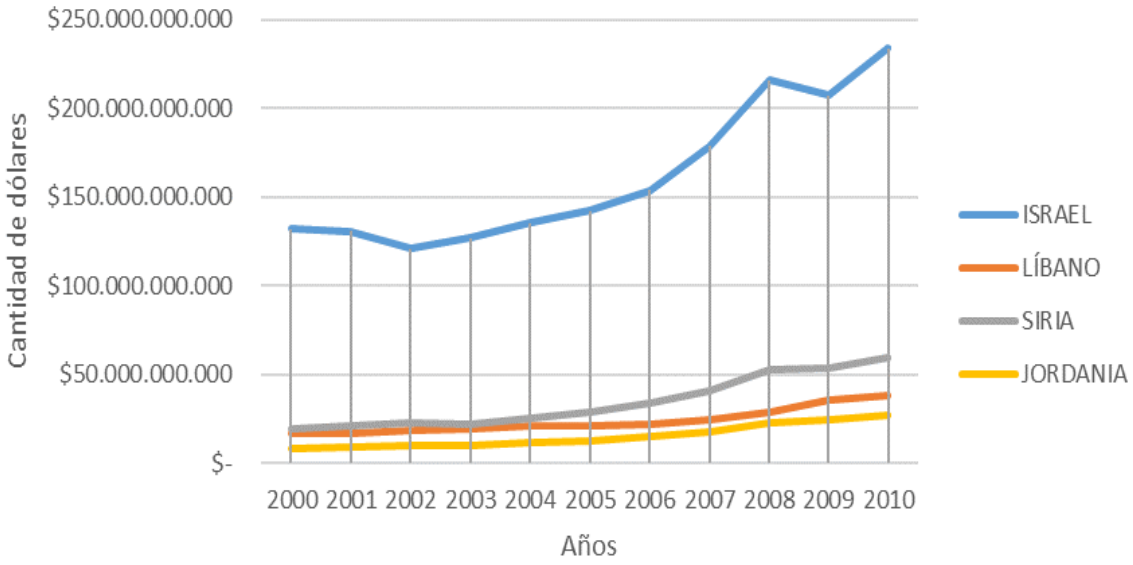
3) Mantener una superioridad económica relativa a sus países vecinos.

Para demostrar lo anterior, se recurrió a un análisis comparativo de las cifras macroeconómicas de Israel y sus países vecinos desde el año 2000 hasta el año 2010, con el objetivo de identificar los efectos de la guerra del año 2006. En segundo lugar, las variaciones en el crecimiento de los países fueron confrontadas con las cifras que cuantifican los daños sufridos por los beligerantes al término de las hostilidades con el objeto de ajustar el margen de error en el impacto de las cifras del crecimiento. Junto a lo anterior, se revisaron las ayudas económicas recibidas por el Líbano por parte de la comunidad internacional al término del conflicto y las cifras de crecimiento evidenciadas en los años posteriores a la guerra.

En el análisis se evidencia que Israel no emplea más del 2% de su capacidad militar en forma simultánea. Lo anterior, sumado a los daños provocados en ambos países se puede determinar que en el caso de Israel logró generar un nivel de daños económicos similar al que Hezbollah ocasionó a Israel pero con el empleo de casi el 100% de su capacidad militar. Por lo tanto, la relación costo/beneficio en esta campaña es contundente y beneficia a Israel.

Gráfico 3

Producto Interno Bruto Países del Medio Oriente



Nota. Elaboración propia a partir de datos extraídos del sitio web https://countryeconomy.com

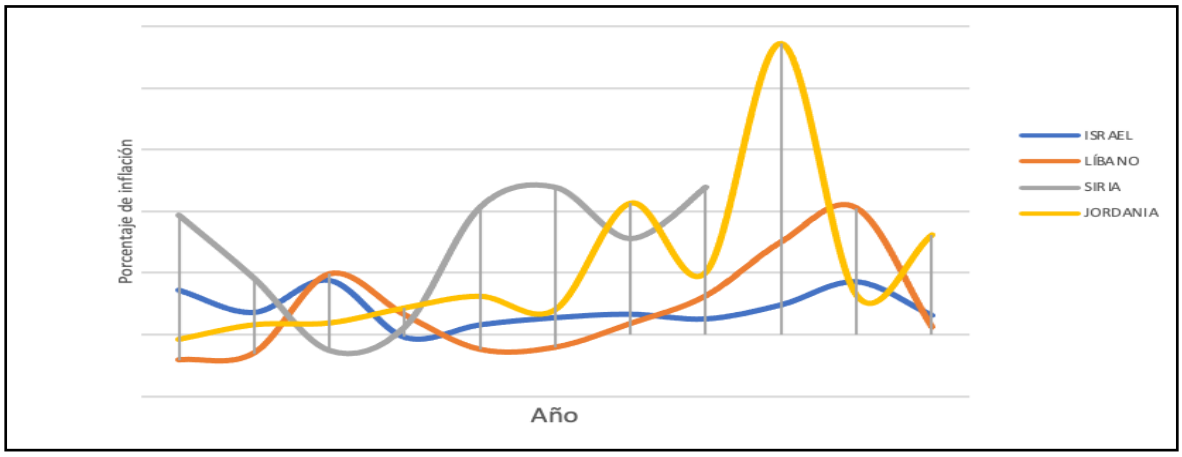
Por otro lado, cuando se analiza las cifras macroeconómicas Israel, sin ningún tipo de ayuda más que la cooperación histórica que ha tenido con EE.UU., logró mantener su economía estable conforme a lo que venía presentando los años anteriores. Además, al emplear una baja capacidad militar durante el conflicto (Merom, The Second Lebanon War: Democratic Lessons Imperfectly Applied, 2008), no tuvo que invertir mayormente en rearmar su Ejército; aspecto que, no es comparable con los daños sufridos por Hezbollah, donde, aparte de haber perdido su influencia en el territorio donde desarrollaban sus actividades, tuvo que armarse nuevamente con el apoyo de otros países, como Irán (Henriksen, 2012).

Ambos aspectos mencionados, demuestran una relación positiva y favorable en cuanto a la eficiencia del empleo de los recursos por parte de Israel, mientras Hezbollah emplea gran parte de su arsenal militar en un conflicto que es iniciado en búsqueda de alcanzar un objetivo menor, que excede sus costos, como lo fue la recuperación de prisioneros.

Por otro lado, Israel no solo ocupa una menor proporción de sus recursos militares y económicos, sino que además logra a un bajo costo disuadir futuros ataques, manteniendo la paz y estabilidad en la zona norte durante los cinco años posteriores al cese del fuego. Para cualquier Estado el desarrollo de una campaña militar tiene efectos nocivos en su economía. La disminución del crecimiento, el impacto en la industria, en la población y en otros factores productivos desencadenan una serie de dificultades que el Estado debe solucionar antes, durante y después del desarrollo del conflicto. Sin embargo, el caso de Israel no se ciñe a la norma, lo que permite inferir una eficiente planificación del gasto para enfrentar la guerra del año 2006.

Gráfico 4

Variación de la Inflación



Nota. Elaboración propia a partir de datos extraídos del sitio web https://countryeconomy.com

Los daños producidos durante la guerra en su territorio ascienden a US$1.400 millones, según los datos entregados por la Cámara de Comercio de Israel (MFA Israel, 2013). Para Israel el costo sería significativamente menor, si solo se toman los datos más optimistas (US$1.144 millones Líbano y $1.400 millones Israel). El porcentaje de los daños equivalentes en el PIB de Israel sería de un 0,9% contra el 5,17% del Líbano. Sin embargo, al momento de considerar otros factores asociados a la capacidad de un país de soportar los efectos de una guerra como ésta, Israel logra una posición más favorable.

Ahora bien, si contrastamos los resultados obtenidos del análisis de Israel con la realidad enfrentada por el Estado libanés, podemos observar la relevancia que la intervención internacional significó en el futuro del país árabe. En este sentido, el nivel de daño en el Líbano generado por la guerra es de aproximadamente USD 1.144 millones, la destrucción de la guerra debilitó todos los sectores de la economía libanesa (Darwish, Farajalla, & Masri, 2009).

Otro estudio cifra los daños en aproximadamente USD 2.805 millones (Haddad & Okuyama, 2016), particularmente, el daño directo e indirecto a la agricultura y su producción fue estimada en USD 18.300 millones (Darwish, Farajalla, & Masri, 2009).

Como se aprecia en el Gráfico 4, el Líbano no habría sufrido más efectos en su economía que la subida de su inflación de un 0,8% el año 2006 a un 10% el año 2009.

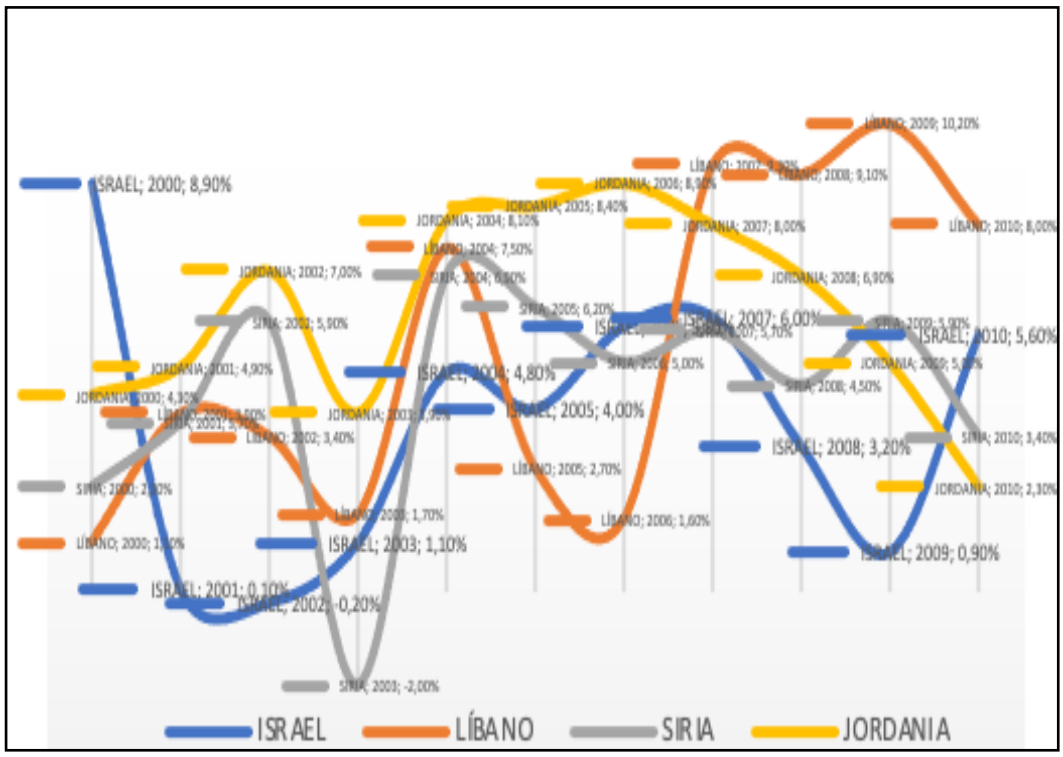
Según la información señalada en el Gráfico 5, Israel habría tenido una caída en su crecimiento, representada por la variación del PIB. Sin embargo, se deben considerar que, por un lado, el PIB de Israel es casi siete veces mayor que el del Líbano, manteniéndose esta proporción relativamente estable, además la aparente baja de Israel estuvo también influenciada por la crisis Subprime de los años 2007 y 2008; por otro lado, en el caso del Líbano se muestra un aumento drástico en su PIB los años posteriores a la guerra, cercano al 10%.

Esto se explicaría principalmente por la influencia ejercida por los aportes económicos de la comunidad internacional y donaciones realizadas (Haddad & Okuyama, 2016).

A esto se suma que, la economía libanesa, por sus características, no habría recibido los efectos de la crisis Subprime.

Gráfico 5

Variación porcentual del PIB



Nota. Elaboración propia a partir de datos extraídos del sitio web https://countryeconomy.com

El análisis permite concluir que Israel logra mantener estable su superioridad económica en la región, lo que le permite sostener una posición ventajosa en cuanto a su desarrollo militar y social. Generando con esto condiciones de seguridad para su Estado, fortaleciendo su supervivencia. No obstante, se debe destacar que la alta resiliencia demostrada por el Líbano para enfrentar una crisis socioeconómica producto de la guerra, hacen creer que de no haber enfrentado una guerra con su vecino del sur el año 2006, sus índices económicos podrían haber sido aún más altos y favorables, siempre y cuando la ayuda internacional se hubiera mantenido estable, sobretodo producto de las conferencias de París los años 2001 y 2002 (Galdon Clavell, 2007), a la que se suma la conferencia Paris III en el año 2007, la que alcanzó un monto de USD 7.600 millones que se sumaron a los USD 1.200 millones que se entregaron posterior a la guerra el año 2006 (Rached, 2006). Estos recursos, no serían del todo “extraordinarios” para el país, ya que recibir ayudas ha sido una

constante, así, no existen antecedentes que hubieran hecho presagiar que las ayudas del extranjero no se hubieran realizado sin guerra.

La resiliencia económica mostrada por el Líbano, sumado a las ayudas recibidas podrían haber incrementado su crecimiento económico intentando romper la relación 7:1 que tiene con Israel; sin embargo, ello no ocurrió.

REFLEXIONES FINALES

Se puede observar que el conflicto entre Israel y Hezbollah en el año 2006, no solo tuvo los alcances propios de un combate militar que duró 33 días, sino que dejó diversas lecciones desde el punto de vista diplomático, militar, económico y de la información. Dichos aspectos analizados permiten realizar una reinterpretación de los hechos acontecidos que, en su conjunto, hacen plausible la afirmación de que Israel no fue derrotado en la guerra del Líbano del año 2006.

En el ámbito diplomático, se evidencia el éxito en el manejo de las relaciones internacionales por parte de Israel. A saber, su empleo desde el inicio de las hostilidades con el objetivo de obtener el apoyo de sus aliados estratégicos, apoyo obtenido de su principal aliado EE.UU, le dieron una ventaja considerable a la hora de negociar consecuencias del conflicto.

No obstante, las visiones particulares de cada instrumento del poder nacional y su demostración de éxito, no habrían sido posible sin existir una correlación armónica en la articulación de éstos. El corolario de lo expuesto se da en la decisión de no invadir el sur del Líbano; sin embargo, influyó positivamente en algunos instrumentos del poder nacional.

En este sentido, la diplomacia fue clave para la obtención de apoyo de los organismos internacionales; de lo contrario, la imagen del país se hubiera deteriorado al haber sido considerado un país “invasor” y se habría afectado el ambiente de la información dando la razón a los que se oponían a la guerra, asumiendo todo el costo moral de los hechos. En el ámbito militar, el costo que se debería haber asumido es de alcances incalculables, una ocupación de esas características hubiera demandado el empleo de más fuerzas militares. Por último, los costos económicos de invadir y

hacerse cargo de la situación socioeconómica del terreno obtenido, habrían hecho de esta guerra una empresa poco rentable.

Al analizar el desempeño de Israel en los conflictos, se debe siempre tener en cuenta su interés nacional de supervivencia, la seguridad de sus fronteras es prioridad y en ese contexto desarrolla su estrategia de disuasión. Israel es un país permanentemente amenazado por sus vecinos árabes, por lo que la paz en la frontera norte durante cinco años es considerado un triunfo importante, tanto para su seguridad, como para el desarrollo de su Estado y población.

Por lo anterior, se estima que Israel no fue derrotado. En este sentido, logró articular su poder y mantenerlo a un costo razonable, lo que le permitió seguir viviendo en un ambiente seguro y con un desarrollo económico estable a pesar de lo volátil de sus vecinos. La historia sigue demostrando que amenazar a Israel no es y no será fácil, ya que la supervivencia del país siempre se sobrepone a otros intereses, lo cual es consecuencia de una correcta armonía en la articulación de los instrumentos del poder nacional.

REFERENCIAS

Amado, V. M. (2006). *Las consecuencias de la guerra contra Hezbolá en Israel.* Madrid: Real Instituto Elcano.

Barnea, N. (2006). Israel vs Hezbollah. *Foreign Policy, 157*, 22-28.

Darwish, R., Farajalla, N., & Masri, R. (2009). The 2006 war and its inter-temporal economic impact on agriculture in Lebanon. *Dissasters, 33*(4), 629-644.

Escuela Superior de Guerra Conjunta de las Fuerzas Armadas. (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 2006.* Buenos Aires.

Galdon Clavell, G. (2007, Marzo 01). *Líbano: "Donaciones" envenenadas*. Retrieved from TNI: https://www.tni.org/my/node/10014?content_language=es

Giaquinta, J. (2009). Estudio del conflicto armado Israel-Líbano durante el año 2006 desde conceptos teóricos de las relaciones internacionales. *Boletín del Centro Naval*, 75-88.

Glenn, R. W. (2012). *All Glory Is Fleeting: Insights from the Second Lebanon War*. Retrieved.

Haddad, E., & Okuyama, Y. (2016). Spatial Propagation of the Economic Impacts of Bombing: The Case of the 2006 War in Lebanon. *Review of Middle East Economics and Finance, 12*(3), 225-256.

Hass, R. (1995). *Military intervention: a taxonomy of challenges and responses.* Maryland: The Aspen Institute.

Henriksen, D. (2012, Febrero 24). Deterrence by Default? Israel's Military Strategy in the 2006 War against Hizballah. *Journal of Strategic Studies, 35*(1), 95-120.

International Institute for Strategic Studies. (2007). *Military Balance.* Londres: Taylor & Francis Group.

International Institute for Counter-Terrorism. (1988). *The Hizballah Program an Open Letter.*Jerusalem: International Institute for Counter-Terrorism.

Jewish Virtual Library. (2008, Enero 31). *Second Lebanon War: The Winograd Commission*. Retrieved from Jewish Virtual Library: https://www.jewishvirtuallibrary.org/background-and-overview-second-lebanon-war

Liddell Hart, B.H. (1967). *Strategy*. Faber & Faber.

Luttwak, E. (2005). *Parabellum: La estrategia de la paz y de la guerra.* Madrid: Siglo XXI de España Editores S.A.

Merom, G. (2008, Marzo 21). The Second Lebanon War: Democratic Lessons Imperfectly Applied. *Democracy and Security, 4*(1), 5-33.

MFA Israel. (2013, Enero 01). *The Second Lebanon War (2006)*. Retrieved from Israel Ministry of Foreign Affairs: https://mfa.gov.il/mfa/foreignpolicy/terrorism/hizbullah/pages/hizbullah%20attack%20in%20northern%20israel%20and%20israels%20response%2012-jul-2006.aspx

Morgentahau, H. (1986). *Política entre las Naciones. La Lucha por el Poder y la Paz.* Buenos Aires: Grupo Editor Latinoamericano SRL.

Rached, C. (2006, Diciembre 01). *La "III Conferencia de Paris" y la Agenda de Reformas*. Retrieved from Social Watch: Erradicación de la pobreza y justicia de género: https://www.socialwatch.org/es/node/10541

Russel, G. (2021). *All Glory Is Fleeting: Insights from the Second Lebanon War*. RAND Corporation. http://www.jstor.org/stable/10.7249/j.ctt3fh003

Seib, P. (2007). *New Media and the New Middle East. New York*. Palgrave Macmillan ed.

UNSC. (2006, Agosto 11). *ODS - Sédoc*. Retrieved from Official Documents System of the United Nations: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N06/465/06/PDF/N0646506.pdf?OpenElement

UNSC. (2006). *Security Council calls for end to hostilities between Hizbollah and Israel, unanimously adopting the resolution.* Nueva York: Department of Public Information-News and Media Division.

ANÁLISIS HISTÓRICO DE LA BATALLA DE KURSK 1943 (OPERACIÓN CIUDADELA): ¿FUE UNA BATALLA DECISIVA EN EL FRENTE ORIENTAL?

Historical Analysis of Kursk 1943 (Operation Citadel): ¿Can it be considered as a Decisive Battle on the Eastern Front?

Carlos Stange Pooley*

Resumen: Finalizada la Segunda Guerra Mundial, las ideologías, nacionalismos e influencia que cada país beligerante tuvo en el esfuerzo realizado para derrotar al Eje han causado distorsiones e imprecisiones. En este sentido, cada uno ha dado a conocer su perspectiva de los hechos históricos. La confrontación entre alemanes y soviéticos en el Frente Oriental no es la excepción. De los hechos de armas ocurridos en ese escenario, la operación Ciudadela, la ofensiva alemana de 1943 en Kursk, es quizás uno de los más controvertidos e incomprendidos. La mayoría de la literatura afirma que se trata de una batalla decisiva, que inclinó la balanza en favor de los soviéticos. Sin embargo, algunos autores no le dan esa relevancia. Este artículo busca determinar la trascendencia de esta contienda en la victoria final soviética y si fue realmente una batalla decisiva.

Palabras claves: Segunda Guerra Mundial, frente oriental, operación ciudadela, Kursk, batalla decisiva

Abstract: After World War II, there have been different interpretations, as each belligerent country has told the story according to its perspective. As a result, misunderstandings and misinterpretations of history have occurred. Especially in the confrontation between Germans and Soviets on the Eastern Front. Citadel, the 1943 German offensive in Kursk, is perhaps one of the most controversial episodes. Most of the scholars assert that this is a decisive battle, which tipped the balance in favor of the Soviets. However, some authors do not give it that

* Abogado. Magíster en Historia Militar y Pensamiento Estratégico, Academia de Guerra del Ejército y Magíster en Derecho de la Empresa. ✉cstange@yarurstange.cl

relevance. Therefore, this article seeks to determine the significance of this contest in the final Soviet victory and if it was really a decisive operation.

Key words: World War II, eastern front, citadel operation, Kursk, decisive battle

INTRODUCCIÓN

La batalla de Kursk[1], durante el verano de 1943, es considerada la confrontación más grande de la Segunda Guerra Mundial. Ambos bandos desplegaron más de 4.000.000 soldados, 69.000 piezas de artillería, 13.000 blindados y 12.000 aviones. Las bajas ascendieron a 685.456 hombres y 6.064 carros de combate para los soviéticos; y, para los alemanes, 340.994 y 1.300 respectivamente (Glantz y House, 1999; Zetterling y Frankson, 2000).

La génesis de esta batalla se remonta a la invasión por parte del Tercer Reich a la Unión Soviética en 1941. En 1942 Alemania lanza una nueva campaña focalizada en los recursos naturales del Cáucaso, la que terminó con la derrota en Stalingrado. Las contraofensivas soviéticas que siguieron, amenazaron la sobrevivencia de los ejércitos alemanes al sur de Rusia. El fin de las operaciones dejó al Ejército Rojo en posesión del denominado saliente de Kursk, el cual penetraba profundamente en el frente germano. En ese sector los alemanes concentraron sus esfuerzos para la próxima campaña, la cual llamaron Operación Ciudadela. Esta última, ha sido objeto de versiones encontradas en la literatura, haciendo de Kursk una de las batallas más controvertidas de la guerra. La mayoría de los autores postulan que sus consecuencias fueron decisivas para la victoria soviética en el Frente Oriental[2]. Sin embargo, algunos no les dan esa relevancia. Por ejemplo, para el mariscal Zhukov (2013) esta batalla es una de las más grandiosas de la Segunda Guerra Mundial; para Overy (1995) es una batalla

[1] Kursk comprende tres operaciones superpuestas: La ofensiva germana Ciudadela (5 al 16 de julio), y las siguientes ofensivas soviéticas Kutusov (12 de julio al 18 de agosto) y capitán Rumyantsev (3 al 23 de agosto).

[2] Frente de Europa Oriental o Frente Oriental, abarcó el centro y este de Europa y fue abierto por Alemania y sus aliados el 22 de junio de 1941 (Thomas, 1999).

decisiva[3] como lo fue Waterloo. No obstante, Frieser (2017) considera aberrante darle esa categoría, tanto porque los objetivos alemanes solo pueden ser calificados de limitados y sus pérdidas no fueron, por sí solas, decisivas para la guerra.

El presente artículo discute la relevancia que la Operación Ciudadela tuvo para la victoria soviética en el Frente Oriental, buscando determinar sus reales efectos y si estos permiten catalogar específicamente a la batalla de Kursk como decisiva. Para ello, se describe de manera general el contexto histórico. Posteriormente, se abordan diversos aspectos militares de la Operación Ciudadela, prestando especial atención en los objetivos de los contendientes, la situación cualitativa y cuantitativa de sus fuerzas, las razones que los alemanes tuvieron para cancelar su ofensiva y las consecuencias de esta decisión. Finalmente, se presentan las conclusiones que permiten determinar la relevancia de la operación.

Para realizar este artículo se ha efectuado una selección bibliográfica, sustentada en publicaciones que plantean diferentes miradas sobre la Operación Ciudadela y material técnico referente a las fuerzas involucradas, sus medios, utilización y desempeño. Adquieren particular relevancia como fuentes primarias memorias de algunos de los principales generales involucrados en dicha operación, tales como vonManstein, Guderian, Rokossovsky y Zhukov. Respecto de las fuentes secundarias, se han escogido publicaciones de autores de diversas nacionalidades y distintas miradas, destacando las obras de Carell, Forczyk, Zamulin, Frieser, Glantz, House, Healy, Töppel, Jukes, Nipe, Overy y Showalter, entre otras. Los aspectos específicos sobre las fuerzas enfrentadas, su liderazgo, inteligencia, doctrina, táctica y pérdidas provienen de autores referentes sobre estas materias, tales como Zaloga, Thomas, Doyle, Jentz, Chamberlain, Liddell y

[3] La batalla decisiva, según Liddell, (2014), aun cuando sea la única meta, se debe reconocer que el objetivo de la estrategia es librar dicha batalla bajo las circunstancias más ventajosas y mientras más lo sean, proporcionalmente menor será el combate. Von Clausewitz (2005), afirma "…siempre se le contemplará como el verdadero centro de gravedad de la guerra, y de ahí su carácter distintivo, de que está ahí por sí misma más que ningún otro combate" (p.223). Para Jomini (2008), el punto decisivo era aquel que, con su ataque o captura, provocaría un serio peligro al enemigo o le debilitaría gravemente.

Schneider. Esta discusión bibliográfica permite tener una visión más clara de los distintos puntos de vistas sobre la batalla y las consecuencias de ésta para el devenir de la contienda entre alemanes y soviéticos.

CONTEXTO HISTÓRICO

En 22 de junio de 1941 Hitler ordena a la Wehrmacht[4] ajustar cuentas con el coloso soviético e inicia la Operación Barbarroja. La Unión Soviética es sorprendida a todo nivel, incluso Stalin creía que el ataque era instigado por algunos generales alemanes (Zhukov, 2013). El resultado fue catastrófico, millones de soldados y enormes extensiones de territorio cayeron en manos del invasor. Finalmente, la campaña fracasó a las puertas de Moscú, alejando toda posibilidad de lograr que el gobierno de Stalin colapsara.

El agotamiento, problemas logísticos, las bajas, la incapacidad del Alto Mando alemán de fijar objetivos alcanzables, el haber subestimado la estabilidad del régimen soviético, su capacidad industrial[5], la resiliencia de su ejército, el clima y la extensión del territorio le pasaron la cuenta al ejército alemán. A ello se sumó la encarnizada resistencia rusa y el invierno que vino a cobrar su cuota. También, cabe destacar, que los alemanes repetían una y otra vez las maniobras de envolvimiento y aniquilación, pero ya el Frente Oriental mostraba claramente que los soviéticos estaban lejos de ser vencidos en una batalla decisiva (Kirchubel, 2007). Para empeorar las cosas, Hitler declara la guerra a los Estados Unidos de América, que, aliado ahora al Reino Unido y a la Unión Soviética, lo enfrenta a las tres potencias industriales del mundo en un combate en que la fuerza militar dependía del potencial económico (Murray y Millet, 2004). Cabe destacar que el denominado programa de “préstamo y arriendo”, iniciado por los estadounidenses antes de su entrada en la guerra, fue vital para los soviéticos, no únicamente en tanques, sino que también en materias primas (el 60% del aluminio utilizado por estos provenía de Estados Unidos de América, sin contar otros minerales, miles

[4] En 1935 Hitler abolió a la Reichswehr y las reemplazó por las nuevas fuerzas armadas, la Wehrmacht (Thomas, 1997).

[5] Los soviéticos logran reubicar 1.500 de sus fábricas estratégicas en los Urales durante 1941 (Davies, 2006).

de toneladas de combustible y maquinas herramientas), aviones y vehículos militares (501.660 camiones y jeeps), que desde 1943 en adelante les permitió llevar adelante sus grandes ofensivas (Zaloga, 2017).

Durante 1942 Alemania se reorganiza y repotencia sus fuerzas, iniciando una nueva campaña de verano, ya no con amplios y ambiciosos objetivos, sino que buscando hacerse de los ricos yacimientos petrolíferos del Cáucaso. Esta campaña, denominada Azul, adolecería de los mismos problemas que la anterior. Finalmente, los alemanes son cercados en Stalingrado, que termina con la rendición del mariscal Paulus y miles de soldados, donde "El enemigo perdió definitivamente la iniciativa estratégica" (Zhukov, 2013, p.781). Esta segunda campaña tampoco logró sus metas estratégicas, pero, lo que es peor, arrebató a la Wehrmacht la iniciativa en el Este. Dicha derrota fue seguida por una serie de contraofensivas soviéticas que empujaron el frente alemán en el sector sur y los obligaron a retroceder.

Von Manstein contraatacó en el momento indicado, evitando el desastre, pero fue detenido por el agotamiento, la rasputitza[6] y los refuerzos enviados apresuradamente por la Stavka[7] (Glantz y House, 1999). El fin de las operaciones dejó a los rusos en posesión del denominado saliente de Kursk[8], en cuyo centro estaba la ciudad del mismo nombre.

CONTEXTO MILITAR DE LA OPERACIÓN CIUDADELA

La Operación Ciudadela tuvo lugar en una amplia extensión de terreno entre las ciudades de Orel, al norte, y Belgorod, al sur, casi en cuyo centro se encuentra la ciudad de Kursk (Ver Mapa 1) en la denominada Meseta de Rusia Central. Esta es una gran planicie con colinas bajas de suaves faldas, profundos barrancos y ríos, que van de Este a Oeste. El clima en verano es muy caluroso y húmedo, pero con imprevistas y fuertes lluvias, lo que dificultó las operaciones aéreas y terrestres (Glantz y House, 1999).

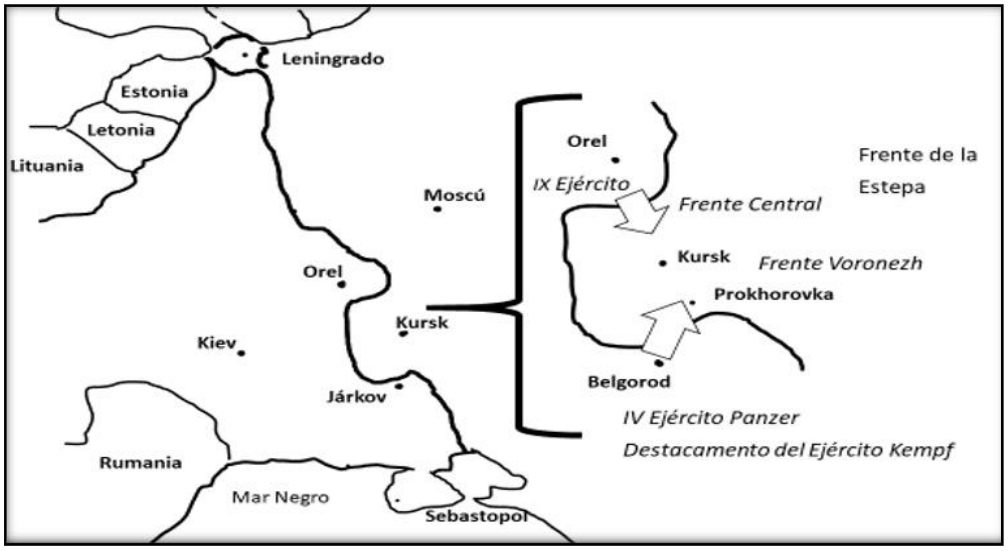
6 La llamada estación del fango en Rusia.
7 Cuartel General Supremo soviético.
8 El saliente tenía 250 km de ancho y 160 de profundidad (Barbier 2002).

En cuanto a la inteligencia de los soviéticos, a diferencia de los alemanes, fueron exitosos a nivel estratégico. El núcleo de sus planes se basó en la información que su red de espías obtenía del Alto Mando germano. Por el contrario, estos últimos nunca pudieron infiltrar la Stavka (Jukes, 1979). De acuerdo al relato de Töppel (2017), y Glantz y House (1999), la inteligencia táctica alemana fue capaz, en parte, de estimar la profundidad y fortaleza de las defensas soviéticas, pero no el número de reservas estratégicas acumuladas, lo que tendría gran impacto en la batalla.

En cuanto a la maniobra, la *Blitzkrieg* o *guerra relámpago* era la base del pensamiento ofensivo alemán, una forma de hacer la guerra que privilegiaba la cooperación entre blindados, aviones, artillería e infantería. Buscaban batallas de encuentro, donde la movilidad y rapidez primaba sobre la potencia de fuego, salvo en aquellos puntos decisivos para producir la ruptura.

Mapa 1

El saliente de Kursk y la ofensiva Ciudadela, 1943



Nota. Elaboración propia.

En 1943 el Alto Mando alemán se mantenía tan atrapado a su tradición del

Kesselschlacht[9], que se habían vuelto ciegos en tratar de lograrlo en Kursk, incluso cuando no había posibilidad de éxito (Citino, 2012). Los soviéticos, por su parte, fueron pioneros en el desarrollo de la estrategia de operaciones sucesivas. Postulaba que los ejércitos modernos eran demasiado grandes para ser derrotados en una batalla decisiva, lo que hacía surgir la necesidad de llevar adelante una serie de ofensivas con fuerzas mecanizadas y, una vez roto el dispositivo adversario, estas debían utilizarse para expandir la brecha y conducir operaciones en la profundidad de la retaguardia enemiga (Glantz y House, 2015). Si bien las purgas de 1937 interrumpieron este pensamiento, oficiales clave como Zhukov y Vasilevsky mantuvieron viva estas ideas.

Según Dunn (2009), el Ejército Rojo en Kursk basó su táctica en la denominada Defensa en Profundidad[10]. La idea era organizar una firme, profunda y escalonada defensa, con una gran cantidad de obstáculos y grupos de choque para lanzar contraataques en caso de rupturas (Glantz, 2014). El foco principal era detener el puño acorazado germano, para lo cual construyeron miles de kilómetros de trincheras, se colocaron miles de minas y obstáculos, se integraron puntos fuertes, hábilmente camuflados y con gran soporte de artillería. Los alemanes, ante la densidad de estas defensas, adoptaron el sistema de Panzerkiel[11], con los carros pesados en la punta, seguidos de carros medianos y la infantería en la base de la formación, mejorando sus posibilidades de penetración (Jukes, 1979). Muchas esperanzas se pusieron en los nuevos tanques, que serían la clave para abrir el dispositivo defensivo soviético (Healy, 2017).

Respecto al mando y control de las fuerzas, Adolf Hitler era el comandante supremo alemán, pero el alejamiento entre este y sus generales desde Stalingardo se había profundizado, apareciendo graves fisuras (Fuller, 1963). El planteamiento de que Hitler tomaba las decisiones sin oír a sus asesores militares hay que

9 Contiene la idea de batallas de envolvimiento o cerco, cuyo objetivo es rodear, matar y capturar al ejército enemigo en el menor tiempo posible (Paret et al., 1991).

10 Se construyeron hasta seis cinturones defensivos, con una profundidad de 120 km (Glantz y House, 1999).

11 Consiste en que dos de las tres compañías del batallón avanzan una al lado de la otra y la restante al frente (Jentz, 1996).

atemperarlo (Citino, 2012). Así, Frieser (2017), critica el hecho de que Hitler, al no tener un órgano único que lo asesorara, terminaba tomando decisiones solo, ya que quedaba al medio de las rivalidades entre el O.K.W.[12] y el O.K.H.[13] La estructura de mando soviética tenía a Stalin como comandante supremo, la Stavka a cargo de las operaciones militares y cada frente tenía asignado un representante de ésta en su Estado Mayor. Stalin, a diferencia de Hitler, desde Stalingrado habría comenzado a reconocer sus limitaciones, dándole mayor libertad de acción a sus comandantes (Clark, 2011).

Las pérdidas de Alemania durante las campañas anteriores disminuyeron la capacidad de combate del ejército y su calidad (Thomas, 1999). La falta de fuerzas, en especial de infantería, durante la Operación Ciudadela obligó a las unidades blindadas a cubrir sus flancos, lo que limitaba capacidad de conquista. La escasez de artillería haría muy importante la actuación de la Luftwaffe en su apoyo a las fuerzas de tierra (Forczyk, 2017a). El Ejército Rojo logró durante 1941 y 1942 movilizar cerca de 400 divisiones[14], ya que, a diferencia de los alemanes, tenía una mayor población en edad militar y más joven. Para 1943 el Ejército Rojo comenzó a reducir la brecha con los alemanes y, como señala Overy (1995), el soldado soviético estaba mejor equipado que nunca. Así para el Ejército Rojo su principal arma era la artillería.

La Luftwaffe estaba en inferioridad numérica, pero se esperaba que lograra la superioridad aérea local sobre Kursk y, posteriormente, pulverizaran las defensas soviéticas en apoyo de los blindados. La calidad de sus pilotos se manifestó en una alta tasa de derribos, pero falló en el reconocimiento aéreo, al no detectar los movimientos de las reservas soviéticas. Al correr los días, y no obstante sus pérdidas, la aviación soviética logró acorralar a su adversario, la diferencia cualitativa entre ambos bandos se iba acortando (Lawrence, 2019).

[12] Oberkommando der Wehrmacht (Alto Mando de la Fuerzas Armadas).
[13] Oberkommando des Heeres (Alto Mando del Ejército).
[14] Los soviéticos movilizaron 700 divisiones durante toda la guerra. Mientras los americanos crearon en 18 meses 100 divisiones, los rusos, en un lapso menor, organizaron más de 500 (Dunn, 2009).

A principios de 1943 la producción alemana de tanques estaba en una situación de caos y la mayoría eran inferiores al T-34 soviético. No obstante, la eficiencia de las tripulaciones y la capacidad de sus oficiales se mantuvieron en un alto estándar. Hitler designa al general Guderian para restablecer la capacidad de combate del arma Panzer (Guderian, 2018). Los nuevos tanques (Tigre y Pantera) significaron un salto tecnológico sobre los aliados. El potente cañón del Tigre podía batir un T-34 fácilmente y su blindaje lo hacía casi invulnerable[15]. Sin embargo, su peso limitaba su movilidad, lo que fue una grave desventaja durante la Operación Ciudadela (Töppel, 2017). Hitler cifró grandes esperanzas en el Pantera. Lamentablemente, fue puesto en producción sin resolver una serie de inconvenientes técnicos, que lo plasmaron de defectos (Nipe, 2017). Ambos solo representaron el 13% de la fuerza, por lo que el peso de la batalla (Ver Tabla 1) recayó en los modelos ya obsoletos III, IV y los cañones asalto, todos inferiores en movilidad al T-34, salvo una leve ventaja de los dos últimos en su poder de fuego (Chamberlain, 1999).

Los soviéticos aún tenían en 1943 grandes cantidades de carros ligeros T-60 y T-70, muy inferiores a los carros alemanes. El T-34/76, el más numeroso en Kursk con casi el 60% de la fuerza (Ver Tabla 2), desde 1941 había sufrido modificaciones menores, ya que se privilegió su producción[16]. Esto hizo que mantuviera defectos de diseño, su cañón perdiera efectividad, lo que, sumado a la falta de equipos de radio, desvaneció su superioridad (Zaloga, 1994). También los soviéticos desplegaron tanques provenientes del programa de Préstamo y Arriendo[17], relegados a apoyo de infantería.

Tabla 1

Blindados alemanes por modelo, Kursk (5 de julio de 1943)

Modelos	Número	%
PzKpfw.* VI (Tigre)	117	5

[15] Según Frieser, (2017), en Ciudadela los Tigre tuvieron solo diez pérdidas totales.
[16] En 1943, de los 19.500 tanques producidos, 16.000 eran T-34/76 (Healy, 2017).
[17] Aunque los efectos de este programa de ayuda aliado a la Unión Soviética fue minimizado durante la Guerra Fría, es indidable que fue un salvavidas (Zaloga, 2017).

PzKpfw. V (Pantera)	194	8
PzKpfw. III	541	23
PzKpfw. IV	666	28
Caza-carros Ferdinand[18]	90	4
Cañones de asalto	565	24
Otros	190	8
Total	2.363	100

Nota. Elaboración propia a partir de datos extraídos de Jentz, (1996), Nipe, (2011), y Zetterling y Frankson, (2000).* Abreviatura: Panzerkampwagen (vehículo acorazado).

Tabla 2

Blindados soviéticos por modelo, Kursk (5 de julio de 1943)

Modelos	Número	%
T-34	2.574	59
T-60 y T-70	1.095	25
KV 1	98	2
SU*	228	5
Otros**	396	9
Total	4.391	100

Nota. Elaboración propia a partir de datos extraídos de: Forczyk (2017b), Zaloga (2017) y Zetterling y Frankson, (2000). *Abreviatura: Samokhodnaya Ustanovka (Cañones autopropulsados) **Otros: programa de Préstamo y Arriendo.

En la producción de blindados los números no favorecían al Reich. Entre 1939 y 1945 fabricaron 26.030 tanques (47.000 si sumamos cañones de asalto, caza-carros, etc.). Los soviéticos alcanzaron la cifra de 105.251 vehículos. Además, los norteamericanos y británicos entre 1939 y 1945 produjeron 88.410 vehículos y 29.288 blindados, respectivamente (Forty, 1996).

¿POR QUÉ KURSK?

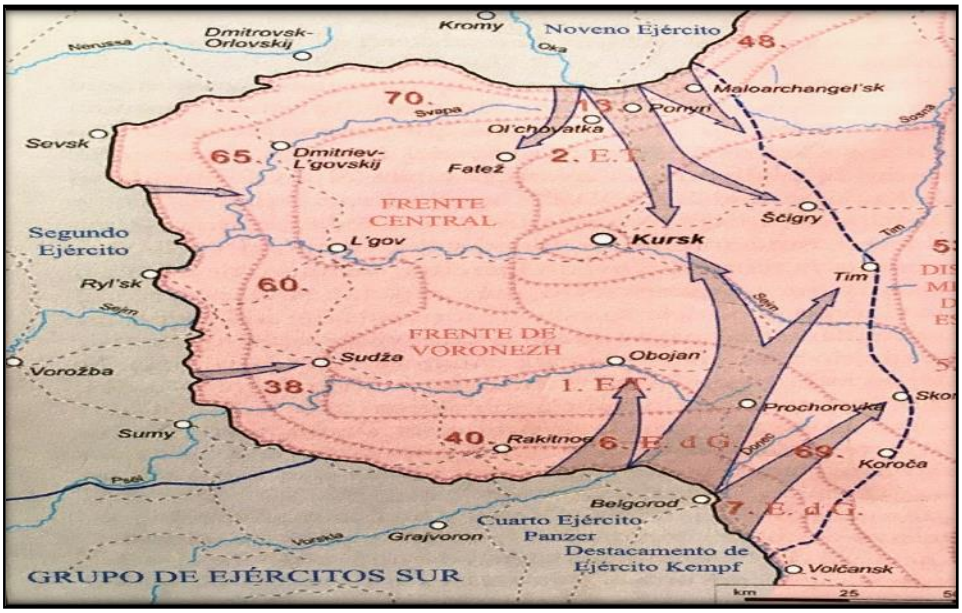
Para 1943 el Reich se enfrentaba a tres grandes potencias, habiendo sufrido duros reveses militares. La postura defensiva era inevitable, pero por razones económicas (recursos naturales) y políticas (estabilidad de sus alianzas) no se contemplaban retiradas a gran escala en el Este. Lo que se buscaba era realizar

[18] En la Operación Ciudadela debutó el caza-carros Ferdinand, por el cual Guderian no compartía el entusiasmo de Hitler, pero sus tripulaciones y la infantería valoraron su capacidad como destructor de tanques y bunkers (Anderson, 2015).

ataques de objetivos limitados para retener la iniciativa, destinados a causar a los soviéticos perdidas que mermaran su capacidad (Frieser, 2017). El saliente de Kursk aparecía como el lugar más obvio para cumplir con las expectativas y con ese objetivo. Si bien a Hitler no dejaba de inquietarle la ofensiva, esta contaba con el apoyo del O.K.H., aun cuando con cada dilación se fortalecía el dispositivo adversario, por lo que la sorpresa y la concentración serían fundamentales.

Mapa 2

Plan de ataque Operación Ciudadela



Nota. Mapa obtenido de Töppel, R. (2017). *Kursk 1943, La batalla más grande de la Segunda Guerra Mundial.*

Por su parte, las preparaciones defensivas soviéticas eran parte de un plan integral de la Stavka, que buscaba literalmente empalar el ataque alemán[19] y, posteriormente, iniciar sendas ofensivas para retomar Orel y Járkov, llamadas Kutusov y Rumyantsev. No fue fácil convencer a Stalin de no cometer el error de adelantarse a los alemanes. Como señala Jukes (2011), es indudable que la red de inteligencia soviética logró dilucidar las intensiones enemigas y afinar sus planes de acuerdo a ello. La Operación Ciudadela ya no contaba con la ventaja de

[19] El informe de Model sobre las defensas soviéticas correctamente concluyó que el saliente era un campo de muerte, preparado solo para desangrar la ofensiva alemana (Nipe, 2012),

la sorpresa. A juicio de von Clausewitz, “sin ella la superioridad en el punto decisivo no es realmente imaginable” (2005, p.164).

LA BATALLA

En el sector sur del saliente de Kursk, el Grupo de Ejércitos Sur del general von Manstein desplegó el IV Ejército Panzer y el Destacamento de Ejército Kempf. Enfrentaban al Frente de Voronezh del general Vatutin.

En el sector norte, el Grupo de Ejércitos Centro del General von Kluge, desplegó al IX Ejército del General Model, siendo su agrupación la más débil. Se enfrentaban al general Rokossovsky, comandante del Frente Central. La reserva soviética la constituía el Frente de la Estepa al mando del General Koniev (Ver Mapa 2). El número de fuerzas empleadas se detallan en las Tablas 3 y 4.

Model a diferencia de von Manstein, no empleó todos sus blindados para penetrar las defensas soviéticas, sino que, el peso de la batalla recayó en la infantería. Este concepto operativo chocó con el rápido avance de los Panzer el primer día. El no explotar esta penetración enviando sus blindados, le hizo perder su oportunidad para lograr la ruptura (Nipe, 2012). Model tomó esta decisión, consciente de la superioridad soviética y de una posible ofensiva de estos en su sector. No tenía fe en la operación, pero cumplió con sus órdenes no exponiendo innecesariamente sus blindados. Al final del día 10 de julio, ya no tiene sentido seguir y ordena detener el ataque y pasar a la defensiva. El 12 de julio la ofensiva Kutusov era iniciada por los soviéticos, terminando con cualquier posibilidad de continuar por parte de Model.

Tabla 3

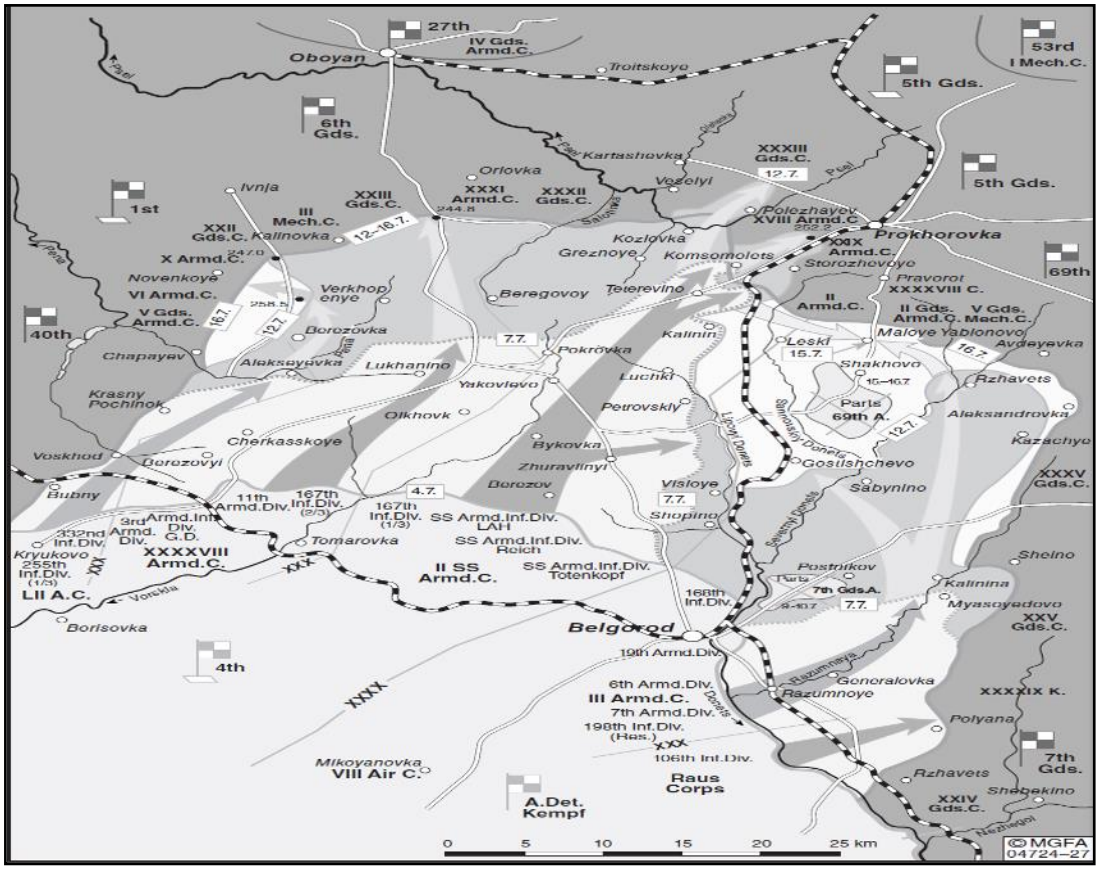
Fuerzas soviéticas empleadas en Ciudadela (5 – 15 de julio de 1943)

	Hombres	Blindados	Cañones	Aviones
Frente Voronezh	625.591	1.704	9.751	881
Frente Central	711.575	1.785	12.453	1.050
Frente Estepa	573.195	1.639	9.211	563
Total	1.910.361	5.128	31.415	2.494

Nota. Elaboración propia a partir de datos extraídos de Frieser (2017) Germany and the Second World War, Volumen VIII, p.100.

Mapa 3

Avance hacia Kursk del Grupo de Ejércitos Sur (5 - 16 Julio de 1943).



Nota. Mapa obtenido de Frieser, K. et al., (2017), en *Germany and the Second World War*, vol. VIII, p.180.

Tabla 4

Fuerzas alemanas empleadas en Ciudadela (5 – 15 de julio de 1943)

	Hombres	Blindados	Cañones	Aviones
IX Ejército (Model)	335.000	920	3.630	730
IV Ejército (Hoth)	223.907	1.089	1.774	1.100
D. Ejército Kempf (Kempf)	108.000	419	1.073	

Total	777.000	2.451	7.417	1.830

Nota. Elaboración propia a partir de datos extraídos de Frieser (2017), en *Germany and the Second World War*, Volumen VIII, p.100.

Von Manstein permitió al general Hoth trabajar un plan táctico para desbordar a los soviéticos en la villa de Prokhorovka. En paralelo, el general Kempf giraría hacia el noreste protegiendo el avance. La maniobra de rompimiento era ineludible, y ante ese dilema la propuesta de Hoth permitía con audacia lograr la sorpresa a nivel táctico (Showalter, 2013). Los germanos atacan la primera línea de defensa, pero su flanco izquierdo sufre graves pérdidas. La misma situación se repite en el flanco derecho al cruzar el río Donets, donde la artillería soviética destruye los puentes impidiendo el paso de los blindados (Töppel, 2017). Solo las divisiones de la Waffen SS logran una penetración significativa, pero la brecha que se fue produciendo con las unidades del ejército les restaría impulso en su avance, al tener que apoyar a las unidades vecinas y proteger sus flancos. Cada uno de los tres cuerpos de ejército alemanes que iban penetrando el frente desarrollaban sus propias batallas privadas (Lawrence, 2019). El quiebre de la tercera línea defensiva significaba que se podría lograr un rompimiento. Healy, afirma que “constituiría una victoria para von Manstein, sin importar cual fuera la suerte del Noveno Ejército al norte del saliente” (2017, p.296). En paralelo los soviéticos movían sus reservas, que habían completado su marcha de 400 km y se organizaban al norte de Prokhorovka[20]. La Luftwaffe falló en detectar estos movimientos, aun cuando se realizaron a plena luz del día.

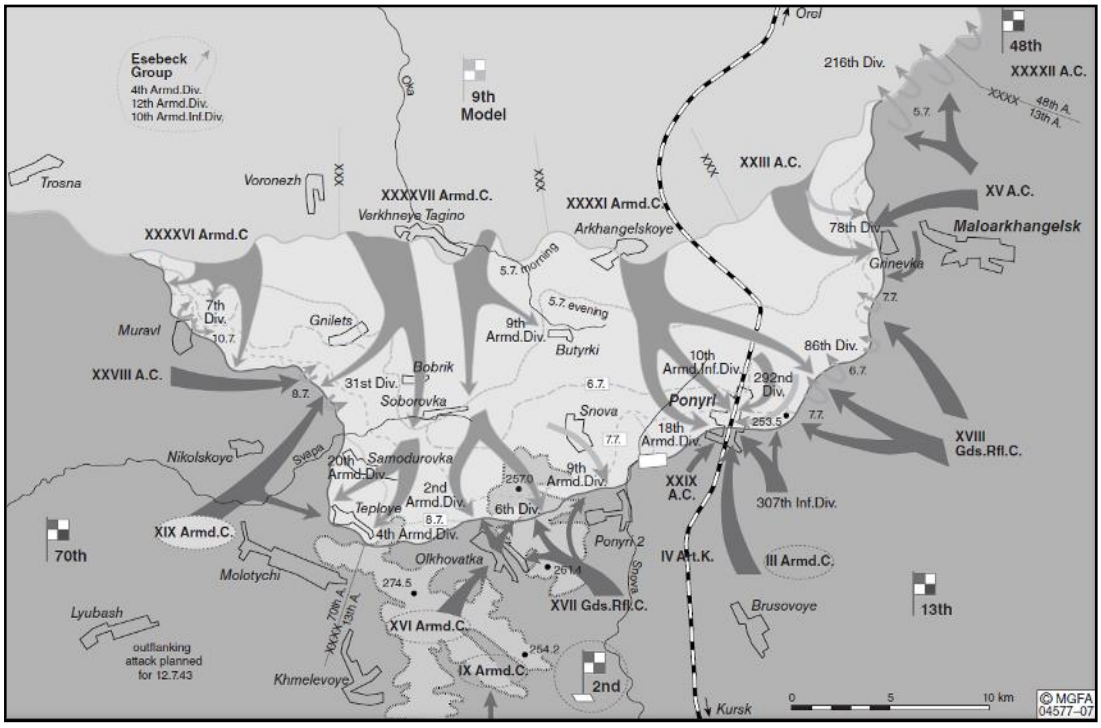
El 10 de julio comienza marcado por acontecimientos que tienen lugar en otra latitud, en Sicilia con desembarco aliado. Esta situación obligó a Hitler a reordenar sus fuerzas para sostener al régimen de Mussolini. No obstante, los éxitos de von Manstein lo incitaron a mantener el curso de la ofensiva. Los soviéticos, por su parte, afinaron los planes para un contraataque, ya que la forma en que avanzaban las puntas de lanza de los Panzer hacia Prokhorovka invitaba a realizar una maniobra de envolvimiento y destrucción. El día 12 de julio lanzan su

[20] Los soviéticos recibían 100.000 nuevas tropas, con 135.000 en ruta, mientras los alemanes no tenían refuerzos (Forczyk, 2017a).

ataque con fuerza, el que sorprende a los germanos. Lamentablemente, una planificación precipitada y falta de coordinación con la artillería y aviación hicieron que los soviéticos se llevaran la peor parte, pero psicológicamente los alemanes fueron noqueados por la escala de la ofensiva soviética y la incertidumbre de lograr sus objetivos (Frieser, 2017).

Mapa 4

El fallido ataque del Grupo de Ejércitos Centro (5 - 11 Julio de 1943).



Nota. Mapa obtenido de Frieser, K. et al., (2017), en *Germany and the Second World War*, Vol. VIII, p.179.

En general se afirma que 1.500 tanques y cañones de asalto soviéticos y alemanes se enfrentaron en Prokhorovka. La cifra real fue de aproximadamente 800 entre ambos contendientes, siendo los alemanes cerca de 300 Glantz y House (1999) y Lawrence (2019).

Koniev bautizó a la batalla de Kursk como el canto del cisne de los Panzer, particularmente por las catastróficas pérdidas sufridas el día 12 de julio[21]. Para los soviéticos la batalla de Kursk se ganó en la batalla de tanques en Prokhorovka (Harrison, 2016). La realidad de las pérdidas alemanas es bastante inferior a lo señalado, siendo las soviéticas catastróficas. Lawrence (2019), Zetterling y Frankson (2000), Nipe (2011), Zamulin (2017), y Frieser (2017) concuerdan en que los germanos perdieron ese día 522 hombres (muertos y heridos) y 63 blindados (17 pérdida total)[22], y el Ejército Rojo 3.563 y 334 (235 pérdida total), respectivamente.

Entonces ¿Cómo Prokhorovka se transformó en una resonante victoria soviética? Todo se debe a un encubrimiento, donde el general Rotmistrov, que lideró el contraataque, volvió la derrota en una victoria. La propaganda soviética moldeó los acontecimientos, hasta quedar plasmados en la historia oficial (Zamulin, 2017). Kursk quedó como la mayor batalla de tanques de la guerra y la victoria que había cambiado el destino de la guerra. El relato, como señal Nipe (2011), se traspasó sin filtro a las siguientes generaciones de historiadores. De hecho, Frieser afirma que “el mito de Prokhorovka como el ‘cementerio de los blindados alemanes´ parece inextirpable” (2017, p. 134).

El 16 de julio las necesidades de otros sectores del frente, y los acontecimientos en Italia, terminaron con la Operación Ciudadela. En efecto, Von Manstein afirma que “ante esta reducción de fuerzas, el Grupo de Ejércitos y su mando se vieron forzados a renunciar a los golpes planeados, a desistir de la acción general y a replegar los ejércitos a las posiciones de partida” (1956, p.459).

Tabla 5

Pérdidas durante la Operación Ciudadela

	Hombres	Blindados	Artillería	Aviones
Wehrmacht	54.182	252	Sin datos	159

[21] Overy, (1995), afirma “Solo el día 12 fueron destruidos más de 300 carros de combate alemanes” (p.114). Otros autores, como Jukes (1979) y Healy (1994), llegan a la misma cifra.

[22] Vehículos que no pueden ser reparados.

Ejército Rojo	319.000 (177.847)*	1.956 (1.614)*	3.929	1.961 (459)*

Nota. Elaboración propia a partir de datos extraídos de Zetterling y Frankson (2000, y Frieser (2017). *Cifras oficiales.

¿Cuál fue el costo final? Podemos afirmar, por los antecedentes examinados, que las pérdidas alemanas durante la ofensiva son bastante menores que las soviéticas.

Sobre los efectos del fracaso de la Operación Ciudadela, las posturas de los distintos autores son contradictorias. Para los generales alemanes, como von Manstein (1956) y von Mellethin (1971), se había perdido la iniciativa en el Este. Guderian (2018) afirma que es una derrota decisiva. Los soviéticos exaltan aún más su éxito. Zhukov (2013) la ve como la batalla más grandiosa de la guerra. Rokossovsky (2007) afirma que “la iniciativa pasó irrevocablemente a manos de nuestro mando” (p. 246). Algunos historiadores también remarcan su importancia, así Overy (1995), Davies (2006) y Carell (1970) ven en Kursk un punto de inflexión en la guerra del Frente Oriental. La calificación de esta como la batalla decisiva es recurrente en sus afirmaciones. Para otros, como Nipe (2012) y Healy (2017) no reviste dichas características. Así, Frieser afirma que “parece aberrante considerar la batalla de Kursk como la batalla decisiva de la Segunda Guerra Mundial, ya que en ese momento el resultado de la guerra se decidió hace mucho” (2017, p.169).

REFLEXIONES FINALES

El efecto de la Operación Ciudadela y específicamente de la batalla de Kursk para el resultado de la guerra en el Frente Oriental no permite aseverar que se trata de un punto de inflexión o decisivo de esta contienda. Aproximándonos conceptualmente a la noción de batalla decisiva y, en el entendido que su efecto fue destruir la capacidad militar alemana y con ello sus medios, para seguir la guerra, la respuesta es indudablemente negativa. Las pérdidas en hombres y material para los alemanes fueron bajas y, en realidad, fue el Ejército Rojo el que llevó la peor parte. Esto sí le causó a este último un daño a nivel estratégico, ya que sus reservas blindadas no pudieron estar disponibles en el número requerido para las ofensivas venideras. Sin lugar a dudas, no afectó en forma concluyente el

resultado de la guerra, pero la alargó varios meses. El objetivo asignado a la Operación Ciudadela tampoco tiene las características de decisivo para los alemanes, por lo que no haberlo conseguido, no hizo variar la situación que tenían antes de iniciarla. Es más, incluso de haber sido exitosa, es poco probable que la guerra en el Frente Oriental hubiese tenido un destino distinto. El gran cambio para Alemania se dio en otra latitud, los eventos en Italia modificaron el panorama estratégico, y desde ese momento el frente occidental aumentaría su importancia para los germanos. Este hecho, se suma a los otros factores expuestos que contribuyeron al fracaso de la Operación Ciudadela, y que fueron la diferencia cuantitativa en favor del Ejército Rojo, la pérdida del elemento sorpresa, el ataque frontal a una fortaleza, los aplazamientos de la ofensiva y el mismo desarrollo de ésta. Por su parte, las ventajas cualitativas de la Wehrmacht solo contribuyeron a alargar la contienda.

De acuerdo a lo anterior, se estima que no contribuyó por sí sola a la victoria soviética, sino que surge de una conjunción de factores, algunos ya presentes en las razones de la cancelación de la ofensiva. Como se analizó al ver las campañas de 1941 y 1942, si hubo una posibilidad de ganar la guerra militarmente para los alemanes, esta se evaporó a las puertas de Moscú. La Unión Soviética, no podía ser conquistada en una batalla decisiva y el resultado de la guerra se resolvió en el momento en que Alemania decidió enfrentar a tres potencias industriales, cuyos enormes recursos la llevarían a una guerra de desgaste para la cual no estaba preparada. Esta batalla se estima que podría haber sido una manifestación de lo que ya se había vislumbrado hace mucho para el Reich, perder la guerra.

REFERENCIAS

Anderson, T. (2015). *Ferdinand and Elefant, Tank Destroyers.* Osprey Publishing Ltd.

Barbier, M. (2002).*Kursk: The Greatest Tank Battle 1943*. MBI Publishing Company.

Beevor, A. (2012). *La Segunda Guerra Mundial*. Ediciones de Pasado y Presente, S.L.

Carell, P. (1970). *Scorched Earth. The Russian-German War 1943-1944***.** Boston-Little, Brown and Company-Toronto.

Chamberlain, P. (1999). *Encyclopedia of German Tanks of World War Two: The Complete illustrated directory of German battle tanks, armoured cars, self-propelled Guns and semi-track vehicles***.** Arms & Armor.

Citino, R. (2012). *The Wehrmacht Retreat, Fighting a Lost War, 1943.* University Press of Kansas.

Clark, L. (2011). *The Battle of the Tanks, Kursk, 1943*. Grove Press.

Davies, N. (2006). *Europa en Guerra 1939-1945.* Editorial Digital, Trivillus.

De Jomini, A. (2008). *The Art of War*. Ontario, Legacy Books Press.

Dunn, W. (2009) *Hitler´s Nemesis. The Red Army, 1930-1945*. Stackpole Books.

Forczyk, R. (2014). *Kursk 1943: The Northern Front.* Osprey Publishing.

Forczyk, R. (2017a). *Kursk 1943: The Southern Front.* Osprey Publishing.

Forczyk, R. (2017b). *Tank Warfare on the Eastern Front 1943 – 1945, Red Steamroller.* Pen &Sword Military.

Fuller, J. (1963) *Batallas Decisivas del Mundo Occidental*. Volumen III, Editor Luis de Caralt.

Forty, G. (1996). *World War Two Tanks.* The Book Package Company Limited.

Frieser, K. et al. (2017). *Germany and the Second World War, Volume VIII. The Eastern Front 1943 – 1944: The War in the East and on the Neighbouring Fronts*. Oxford University Press.

Glantz, D. y House, J. (1999). *The Battle of Kursk***.** University Press of Kansas.

Glantz, D. (2014). *Soviet Defensive Tactics at Kursk, July 1943***.** Pickle Partners Publishing, 2014.

Glantz, D. y House, J. (2015). *When Titans Clashed.* University Press of Kansas.

Guderian, H. (2018). *Panzer Leader.* Reading Essentials.

Harrison, R. (2016). *The Battle of Kursk. The Red Army´s Defensive Operations and Counter-Offensive, July–August 1943, Soviet General Staff.* Helion & Company.

Healy, M. (1994). *Kursk 1943, El rumbo cambia en el Este***.** Ed. Del Prado.

Healy, M. (2017). *Zitadelle. The German offensive against the Kursk Salient 4-17 Julio 1943.* History Press Ltd.

Jentz, T. y Doyle, H. (1993). *Tiger I, Heavy Tank 1942-1945*. Osprey Publishing Ltda.

Jentz, T. (1995). *Panther Tank: The Quest for Combat Supremacy.* Schiffer Publishing Ltd.

Jentz, T. (1996). *Panzer Truppen: The Complete Guide to the Creation & Combat Employment of Germany´s Tank Force 1943-1945*. VOL 1 y 2, Schiffer Publishing Ltd.

Jukes, G. (1979). *Kursk: Encuentro de Fuerzas Acorazadas.* Editorial San Martín.

Jukes, G. (2011). *Stalingrad to Kursk, Triumph of the Red Army*. Pen & Sword, Barnsley.

Kirchubel, Robert. (2003). *Operation Barbarossa 1941 (1), Army Group South.* Osprey Publishing Ltd.

Kirchubel, Robert. (2005). *Operation Barbarossa 1941 (2), Army Group North.* Osprey Publishing Ltd.

Kirchubel, R. (2007). *Operation Barbarossa 1941 (3), Army Group Center.* Osprey Publishing Ltd.

Lawrence, C. (2019). *The Battle of Prokhorovka: The Tank Battle al Kursk, the Largest Clash of Armor in History.* Stackpole Books.

Liddell, H. (2014). *La Estrategia de la Aproximación Indirecta*. http://www.laeditorialvirtual.com.ar**,** Edición Electrónica.

Montt, M. (2010), *La guerra, su conducción, política y estratégica.* ANEPE.

Murray, W. y Millet, A. (2004). *La guerra que había que ganar, Historia de la Segunda Guerra Mundial.* Editorial Crítica S.L.

Nipe, G. (2011). *Blood, Steel and Myth: The II-SS Panzer-Korps and the road to Prokhorovka, July 1943*. RZM Publishing.

Nipe, G. (2012). *Decision in the Ukraine, German Panzer Operations on the Eastern Front, summer 1943.* Stackpole Books.

Overy, R. (1995). *Por Qué Ganaros Los Aliados***.** Editorial Digital: Trivillus.

Paret, P. et al. (1991). *Creadores de la Estrategia Moderna, Desde Maquiavelo a la Era Nuclear*. Traductor y Editor.

Rokossovski, K. (2007). *El deber de un Soldado.* Inédita Ed.

Schneider**,** W. (2000) *Tigers in Combat; Vol I.* J.J. Fedorowicz Publishing, Inc: Winnipeg.

Schneider**,** W. (2005). *Panzer Tactics, German Small-Unit Armor Tactics in World War II.* Stackpole Books.

Shirer, W. (1980). *Historia del Tercer Reich.* Barcelona, Ediciones Océano.

Showalter, D. (2013), *Armor and Blood, The Battle of Kursk, The Turning Point of World War II.* New York, Random House Publishing Group.

Spielberger, W. (2007*). Special Panzer Variants.* Schiffer Publishing.

Thomas, N. (1997). *The German Army 1939-45 (1) Blitzkrieg.* Osprey Publishing.

Thomas, N. (1999). *The German Army 1939-45 (4) Eastern Front 1943-45.* Osprey Publishing.

Thomas, N. (2010). *World War II Soviet Armed Forces (1) 1939 – 41***.**Osprey Publishing.

Thomas, N. (2011). *World War II Soviet Armed Forces (2) 1942 – 43.*Osprey Publishing.

Töppel, R. (2017). *Kursk 1943, La batalla más grande de la Segunda Guerra Mundial.* Ediciones Salamina.

Ureña, G. (2012). *Blitzkrieg, El Concepto*. Atenas Editores.

Von Clausewitz, C. (2005). *De la Guerra***.** Madrid, La Esfera de los Libros.

Von Manstein, E. (1956). *Victorias Frustradas.* Editorial Barcelona.

Von Mellenthin, F. (1971) *Panzer Battles 1939-1945, A Study of the Employment of Armour in the Second World War.* New York, First Ballantine Books Edition.

Zaloga, S. (2017). *Soviet Lend – Lease Tanks of World War II.* Osprey Publishing Ltda.

Zaloga, S. (1994). *T 34/76 Medium Tank 1941-45***.** Osprey Publishing Ltda.

Zaloga, S. y Ness, L. (1998). *Red Army Handbook 1939 – 1945*. Sutton Publishing Limited.

Zamulin, V. (2011). *Demolishing the Myth: The Tank Battle at Prokhorovka, Kursk, July 1943.* UK, Helion& Company: Solihull.

Zamulin, V. (2017). *The Battle of Kursk, Controversial and Neglected Aspects*. UK, Helion& Company: Solihull.

Zetterling, N. y Frankson, A. (2000). *Kursk 1943. A Statistical Analysis***.** Frank Cass Publishers.

Zhukov, G. (2013). *Marshal of Victory. The Autobiography of General Georgy Zhukov.*Pen & Sword.

¿TIENE VALIDEZ APLICAR LOS PRINCIPIOS DE LA GUERRA A LA CONTRAINSURGENCIA?

Do the principles of war apply to the Counterinsurgency?

MAY. Gerardo Hermosilla Acevedo*

Resumen: En este análisis se presentan los principios de la guerra y se revisa la aplicabilidad que tienen en la contrainsurgencia. Inicialmente, se explican los conceptos de principios de la guerra, guerra irregular, insurgencia y contrainsurgencia para, posteriormente, analizar de qué manera pueden ser aplicados en la contrainsurgencia, considerando las especiales condiciones donde se desarrollan este tipo de operaciones.

Palabras Claves: principios de la guerra, guerra irregular, insurgencia, contrainsurgencia

Abstract: This article analyzes the principles of war and discusses their applicability to counterinsurgency. Initially, concepts of principles of war, irregular warfare, insurgency and counterinsurgency are explained. Then, the applicability of principles of war to counterinsurgency is evaluated, regarding the special conditions where this kind of operations takes place.

Key Words: principles of war, irregular warfare, insurgency, counterinsurgency

INTRODUCCIÓN

Los principios de la guerra (PG) son máximas primordiales que guían el accionar de las Fuerzas Armadas y, en este caso particular, a sus comandantes, quienes iluminados por la historia, la doctrina y la experiencia, conducen sus medios para realizar una maniobra aplicando la estrategia militar. En este sentido, los principios de la guerra son los que definen cómo y de qué manera, el comandante empleará

* Oficial del Arma de Infantería. Oficial de Estado Mayor. Magíster en Ciencias Militares con mención en Gestión Estratégica. Profesor Militar de Academia en la asignatura de Táctica y Operaciones. Actualmente se desempeña como Comandante de Unidad de Combate de la Fuerza Terrestre del Ejército. ✉ gerardofhermosillaa@hotmail.com

el poder de combate en el diseño de la maniobra, articulando los modos, medios y fines, para lograr un determinando efecto que permita el cumplimiento de la misión.

Por otra parte, el término guerra irregular, es un concepto que puede ser interpretado subjetivamente. De ahí la importancia de aunar criterios que permitan comprender de mejor forma los conceptos y determinar de qué manera se vincula la contrainsurgencia con los principios de la guerra.

En este contexto, el objetivo de este trabajo es analizar la aplicabilidad de los principios de la guerra a la contrainsurgencia. Para lograr lo anterior, inicialmente se discuten los conceptos de principios de la guerra, guerra irregular, insurgencia y contrainsurgencia. Posteriormente, se analiza cada uno de los principios de la guerra y se determina de qué manera pueden ser aplicados a la contrainsurgencia.

PRINCIPIOS DE LA GUERRA

Conforme a la doctrina del Ejército de Chile, la conducción militar es aquel proceso por el cual se dirige la totalidad de las operaciones militares, las que son regidas por un conjunto de normas doctrinarias, propias de un comandante y sus asesores, con los medios que son puestos a su disposición para dar cumplimiento a la misión recibida (Ejército de Chile, 2019, DD-10001, La Fuerza Terrestre).

Propio de la conducción militar son los *elementos* que la componen, es decir, criterios que permiten hacer viable el proceso de conducción de las operaciones. Estos elementos son *los principios de la guerra, el objetivo, el escenario o campo de batalla y la fuerza*, tal como los plantea el Ejército de Chile en DD-10001 La Fuerza Terrestre, publicado el 2019**.**

De acuerdo a la doctrina, los principios de la guerra son:

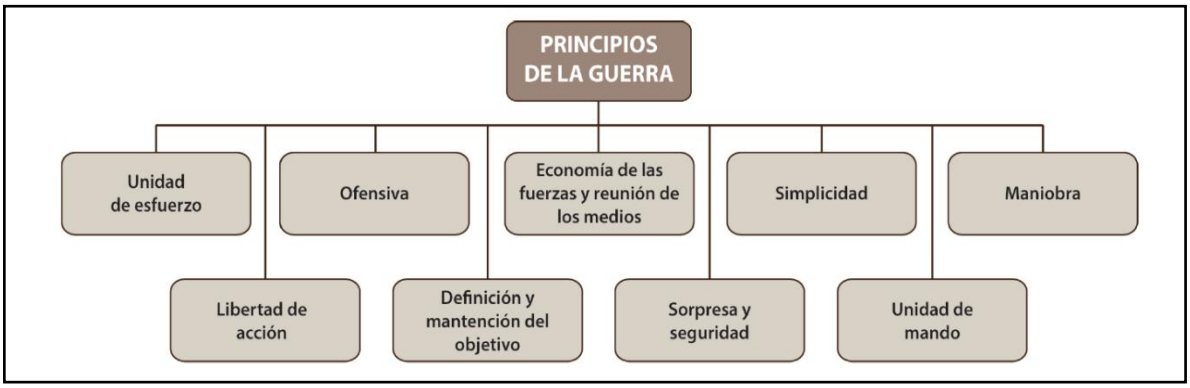
> Basamentos o causas de validez general para la conducción militar, que han sido aplicados por los grandes comandantes y deducidos y analizados por pensadores, estudiosos de la guerra y autores militares a través del

> tiempo, hasta constituir principios en razón a que la historia militar ha demostrado que su reiterada y correcta aplicación, normalmente, ha conducido a los ejércitos a la victoria.
>
> Ellos admiten flexibilidad, por lo tanto, su aplicación requiere de un buen criterio. No son fórmulas que puedan ser aplicadas de la misma manera en todos los casos. En cada oportunidad hay que determinar en qué medida deben o pueden ser utilizados. (Ejército de Chile, DD-10001 La Fuerza Terrestre, 2019, p. 166)

Los principios de la guerra sirven como guía y orientan los procesos resolutivos de los comandantes, siendo válidas en la ejecución, tanto de la guerra como de operaciones militares; por lo que son permanentes en el tiempo:

Figura 1

Los Principios de la Guerra



Nota. Ejército de Chile, 2019, DD -10001 La Fuerza Terrestre, p. 167.

No es cometido de este artículo explicar en detalle cada uno de estos principios. Solo interesa mostrarlos con el fin de contextualizar la relación que podrían tener con el término *contrainsurgencia*.

Remontándonos a la historia, los principios de la guerra más antiguos de los que se tenga conocimiento fueron los elaborados por Sun Tzu aproximadamente en el año 500 A.C. Luego, Nicolás Maquiavelo los describió en su libro “Reglas Generales” publicado en 1521. Como se aprecia, dichos principios han sido de

interés en el desarrollo de la historia militar universal y, puntualmente, en los conflictos armados.

A pesar de ser conceptos doctrinarios y de tener su génesis en las tácticas de la guerra regular o convencional[1], no dictaminan ni la estrategia ni la táctica a emplear por el comandante. De ahí la importancia de separar dichas "máximas" como aplicables según el contexto, considerando que dichos principios tienen su génesis.

Guerra irregular o asimétrica

El RDO-20001 Operaciones (2012, p. 100), define el conflicto armado irregular como "aquel que se produce entre varios contendientes de capacidades militarmente distintas y con diferencias sustanciales en su modelo estratégico". Esto se traduce en que se utilizan tácticas que difieren de las normales y que son propias de la guerra regular. No existe un borde delantero específico ni una determinada acción militar que pueda hacer frente a este tipo de guerra, sino que emplean la totalidad de los elementos del poder nacional para hacerle frente; es decir, una combinación de acciones militares y actividades políticas, económicas, sociales, entre otras, a las que se suma el factor poblacional, donde se desarrolla este tipo de conflicto[2]. Algunos ejemplos de ello son los conflictos en Afganistán, Irak, Israel.

En este tipo de conflictos la población pasa a ser fundamental para las operaciones, teniendo en consideración otros aspectos como son el tecnológico, los medios de comunicación social y los actores políticos, además de la coordinación que deben existir entre todos los medios presentes.

---

1 Es el tipo de guerra en que las fuerzas militares que participan tienen una estructura de mando, organización y equipamiento que las caracteriza como una fuerza institucional al servicio de un Estado - Nación y utilizan procedimientos y sistemas de armas autorizados en las convenciones y tratados vigentes en el derecho internacional (RDO - 20910 Conflicto Armado Asimétrico, 2011, p. 17).

2 Es de naturaleza estratégica y puede ser planteado por actores estatales o no estatales, aunque estos últimos son los mejor adaptados para llevarlo a la práctica. Su finalidad es siempre quebrar la voluntad de un adversario más fuerte, no a través de la derrota de sus fuerzas armadas, sino de la acción sobre su opinión pública (RDO - 20910 Conflicto Armado Asimétrico, 2011, p. 16).

La guerra regular tiene claros indicadores de cuándo se ha logrado la victoria, ya sea porque el adversario ha sido doblegado; se han ganado batallas y la fuerza adversaria ha sido reducida; incluso el oponente ha aceptado su derrota firmando una declaración de rendición. En cambio, en la guerra irregular la derrota militar del oponente no necesariamente es la victoria. En tal sentido, la insurgencia cumple su propósito con el solo hecho de alargar el conflicto e impedir que el Estado la derrote. Por esta razón, la guerra irregular está más vinculada a la capacidad de un grupo determinado (en este caso de un grupo insurgente) de poder obtener el apoyo necesario de la población para alcanzar sus intereses políticos, generalmente de base ideológica. En este caso, el éxito no depende tanto de las capacidades militares, sino que, en la capacidad de poder tener validación y legitimidad ante la sociedad, lo que determina y trae como resultado consecuencias de índole política, que le permiten mantener y dar sustento a su ideología.

Insurgencia y contrainsurgencia

Según el RDO -20910 Conflicto Armado Asimétrico, el término insurgencia es definido como:

> Movimiento violento organizado que emprende una lucha prolongada con la finalidad de cambiar el orden político establecido. Toda insurgencia persigue el poder político. Como medios para lograr sus objetivos se encuentran principalmente la propaganda, la subversión, la presión política y militar y, en su caso, la lucha armada, implicando a la población de forma directa o indirecta. (Ejército de Chile, RDO -20910 Conflicto Armado Asimétrico, 2011, p. 63)

Similar acepción tiene el Joint Chief of Staff of United States of America, JP 3-24 counterinsurgency, definiéndola como:

> El uso organizado de la subversión y la violencia para apoderarse, anular o desafiar el control político de una región. La insurgencia es una forma de conflicto intraestatal. El término insurgencia también puede referirse al

> grupo mismo que la ejecuta. Esta puede combinar el uso del terrorismo, la subversión, el sabotaje y otras actividades políticas, económicas y psicológicas además del conflicto armado para lograr sus objetivos. Es una organización político-militar de lucha, compuesta por un movimiento o grupo predominantemente de población local que está diseñado para debilitar, subvertir o desplazar el control del gobierno establecido de una determinada región. (Joint Chief of Staff of United States of America, JP 3-24 Counterinsurgency, 2018, p. 25)

Ambas fuentes de información señalan que la insurgencia busca cambiar o desplazar al gobierno o control político legítimamente establecido. Como tal, este tipo de acciones se manifiestan principalmente como una lucha política en que las voluntades contrapuestas utilizan tácticas de guerra para crear el espacio necesario para influir en las actividades políticas y económicas logrando así, la eficacia requerida para actuar. Ésta no siempre es dirigida por un grupo con una estructura de mando centralizada, similar a lo militar, sino que presenta diferentes actores con diversos objetivos.

Es por esto que, para lograr el éxito de la insurgencia se requiere de líderes carismáticos, con apoyo de la población, y con una adecuada cadena de suministros, principalmente, de recursos económicos que le permita continuar desarrollando sus actividades. Lo anterior se logra cuando la insurgencia presenta un atractivo político, es capaz de manipular la identidad religiosa, tribal o local para explotar las necesidades sociales que están siendo cuestionadas. Es decir, lograr el control de la población mediante una combinación de persuasión, subversión y coerción, mientras se utilizan tácticas de guerrilla para poder hacer frente y contrarrestar las fuerzas de seguridad del gobierno. La intención final es prolongar la lucha armada, causando un desgaste del gobierno y ganando de esta manera, el suficiente apoyo de la población, para que el gobierno capitule o se adecúe a sus requerimientos.

Por lo tanto, la insurgencia va evolucionando a través de diversas etapas, aunque el desarrollo y la forma en que progresa es diferente caso a caso.

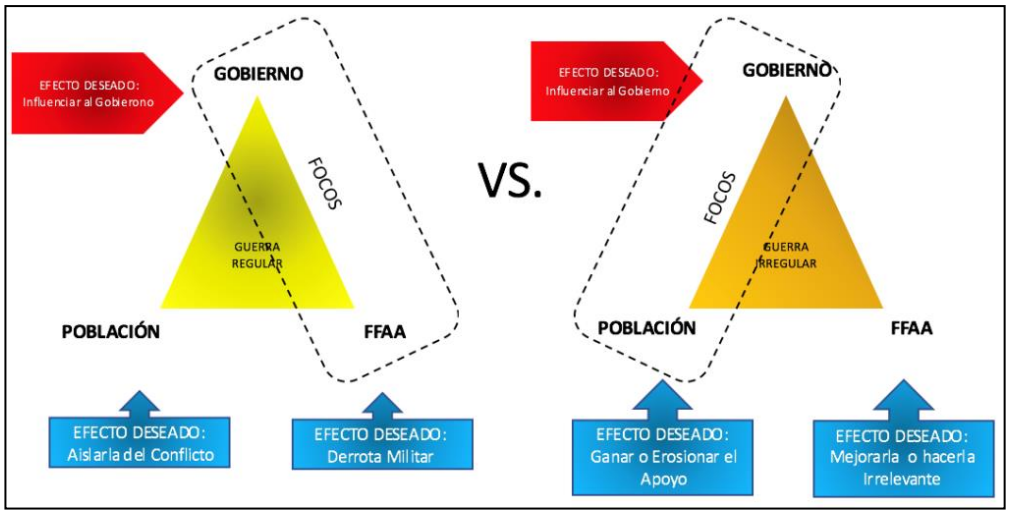
Claramente han existido muchas formas de insurgencia en la historia mundial, las que han tenido una amplia variedad de objetivos político-militares, incluidos los movimientos independentistas contra las potencias coloniales, como la revuelta árabe contra el Imperio Otomano durante la Primera Guerra Mundial y que implicó la ruptura de un imperio multinacional; y, los movimientos revolucionarios marxistas contra regímenes nacionalistas, como por ejemplo, el ocurrido en Laos en el contexto de la guerra de Vietnam, donde la falta de persistencia en el accionar y el término del apoyo brindado por los Estados Unidos significó la derrota; asimismo, en la guerra de Irak y de Afganistán enfrentaron a una fuerza invasora de carácter regular (Fuerzas Armadas de Estados Unidos) contra una fuerza insurgente, la que hacía frente a las fuerzas de la coalición.

Actualmente, en Medio Oriente existe una creciente amenaza de insurgencias islamistas que han adoptado tácticas de "terror". La principal característica de estas, es que poseen tres objetivos político-militares claramente identificables: “eliminar” a Israel; derrocar a los países árabes pro regímenes occidentales y permitir la difusión del Islam radical en todo el mundo para restablecer el Califato (Amidror, 2010).

Etimológicamente, el concepto de contrainsurgencia da a entender que se opone a la insurgencia. Ahora bien, el RDO-20910 Conflicto Armado Asimétrico (2011, p. 63) la define como “conjunto de actividades políticas, diplomáticas, económicas, sociales, militares, de mantenimiento del orden, civiles y psicológicas necesarias para derrotar a una insurgencia”. El concepto en sí, abarca la totalidad de los elementos del poder nacional, teniendo un carácter político; lo que implica que al realizar operaciones de contrainsurgencia debe existir un claro liderazgo para coordinar todos los recursos y medios disponibles para hacer frente a la insurgencia.

Figura 2

Guerra regular versus guerra irregular y su foco de esfuerzo y acción



Nota. US Department of Defense, 2007, Irregular Warfare (IW) Joint Operating Concept (JOC), Version 1.0, p. 08.

A diferencia de la guerra convencional, los medios militares no siempre suelen ser los más adecuados en la lucha contrainsurgente, pero contribuyen a permitir y facilitar dicho enfrentamiento. Las estrategias empleadas, generalmente, irán centradas en la población más que en el enemigo y, buscarán reforzar la legitimidad del gobierno afectado y reduciendo la influencia insurgente. Lo anterior, se logra con aspectos de carácter político que mejoren la gobernanza, así como tomar en cuenta la molestia de la sociedad (donde influye y ataca la fuerza insurgente).

Asimismo, la contrainsurgencia considera otros aspectos además del político, como son lo económico, la seguridad y la información, los que permiten que el gobierno afectado pueda reestablecer el control perdido. Por tanto, se vuelve primordial la sinergia entre todos los medios que participan en hacer frente a la insurgencia. A esto se suma una planificación detallada e integrada además de un proceso continuo de seguimiento, evaluación y valorización que facilite medir el progreso e identificar dónde es necesario efectuar un cambio para lograr el éxito. En definitiva, el estado final deseado es que el gobierno sea considerado legítimo, capaz de tener control político, social, económico y con un ambiente de seguridad

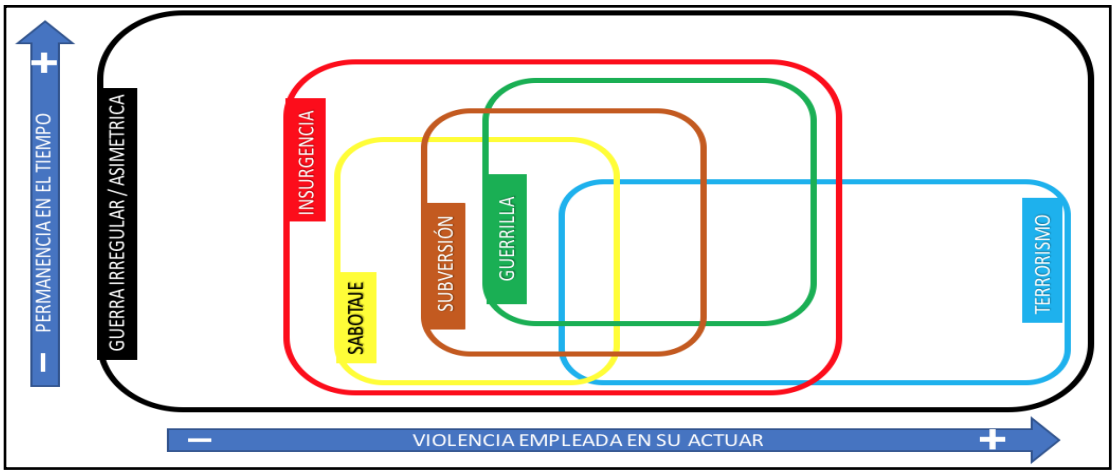
que permita satisfacer las necesidades de la población, incluyendo aquello que en algún momento generó la "causa de lucha" de la fuerza insurgente.

De igual forma existe suficiente evidencia empírica, para afirmar que los ejércitos pueden luchar con cierto grado de éxito contra organizaciones terroristas y guerrilleras, destruyendo sus capacidades operativas, a pesar de que el conflicto permanezca activo en otras áreas.

No obstante, siempre verá mermado su accionar, por factores externos como son los medios de comunicación social o la misma propaganda insurgente que limita el accionar de las tropas militares, por este motivo es que las INFOOPS[3] cobran gran relevancia en la ejecución de la tarea.

Figura 3

Gráfico explicativo de lo que abarca la guerra irregular o asimétrica



Nota. Elaboración propia.

Se debe considerar que el concepto de guerra irregular o asimétrica engloba al concepto de insurgencia, y además a los conceptos de terrorismo, guerrilla, subversión y sabotaje. A pesar de que todos estos conceptos poseen vinculación

[3] Las operaciones de información son realizadas con el fin de afectar el sistema de informaciones adversario y su toma de decisiones y, simultáneamente, proteger el empleo y sistema de información propio. Se desarrollan en apoyo de los objetivos propios, afectando la explotación y protección de la información, los sistemas de mando y control que la soportan y los sistemas de comunicaciones e información que la procesan, a la vez que apoyan y protegen la capacidad propia para obtener, procesar y gestionar la información. De esta forma, se busca influir en las capacidades de decisión del adversario y proteger las propias (RDO-20001 "Operaciones" 2012 p. 70).

no serán definidos aquí, ya que el análisis se debe centrar en determinar la aplicabilidad de los principios de la guerra a la *lucha contra la insurgencia* y si estos tienen pertinencia en la actualidad.

APLICACIÓN DE LOS PRINCIPIOS DE LA GUERRA EN LA CONTRA INSURGENCIA

a. Definición y mantención del objetivo

Este principio es fundamental para cada acción militar. Constituye la realización de las acciones militares en pos de quebrantar la voluntad de lucha del adversario (DD-10001 La Fuerza Terrestre, 2019). Requiere tanto que la misión sea clara y, a partir de ésta, el objetivo bien identificado y definido, permitiendo con ello, asegurar su cumplimiento.

Diversas experiencias históricas muestran que cada vez que una misión no estaba bien definida y no tenía sus objetivos claros, generaba consecuencias negativas para la fuerza, por ejemplo, en la 2da Guerra del Líbano y las consecuencias sufridas por la fuerza Israelita[4].

Este principio requiere que cada comandante use la fuerza que le fue determinada para poder cumplir su misión, teniendo el objetivo claro y bien definido al momento de cumplirla. En cualquier nivel de la conducción militar, el objetivo se desprende de la tarea asignada por el escalón superior y sirve para orientar el cumplimiento de la misión.

En las operaciones de contrainsurgencia, el objetivo se encuentra asociado a la protección de la población, aislándola de los insurgentes que buscan ganar su apoyo a fin de alargar el conflicto y alcanzar sus intereses. Por tanto, cualquier

[4] La 2da Guerra del Líbano fue un conflicto que se extendió desde el 12JUL2006 hasta el 14AGO2006, entre Israel y el brazo armado de la organización Chií Hezbollá, desarrollado en el Libano, norte de Israel y los Altos del Golan. En dicha guerra destacó el uso exitoso de tácticas bélicas asimétricas por parte de Hezbola frente a un adversario tecnológicamente superior como era Israel. Asimismo muchos analistas militares han considerado esta guerra como una derrota para Israel (en La Guerra del Líbano de 2006 y la Evolución de las Tácticas Terrestres Iraníes, *Military Rewiew*, Julio – Agosto 2010).

acción que se ejecute debe estar orientada a ello y a disminuir al máximo el daño colateral.

Figura 4

Principio de definición y mantención del objetivo

Nota. Elaboración propia.

A modo de ejemplo y, a nivel táctico, si los insurgentes han abandonado sus bases seguras desde donde operan, es preferible atacarlos a ellos, como grupo, antes que realizar el ataque a la base, la que había sido definida previamente como la misión a cumplir. Es decir, si la misión es atacar la base, se debe entender y comprender por qué debe realizarse, en este caso, porque existe una fuerza insurgente en su interior, pero si la base se encuentra desocupada ya no tiene sentido atacarla.

Esto difiere de la concepción que se tiene con una situación similar en la guerra regular, donde la misión de conquistar una cota que se encuentra en manos de una fuerza enemiga, obliga al comandante a ocuparla a pesar de que la fuerza adversaria ya no se encuentre en el lugar. Se hace evidente entonces, que la conquista de la cota declarada e impuesta en la misión, independiente que exista o no la fuerza, pasa a ser el objetivo propio y es el que se debe alcanzar con la operación.

b. Economía de las fuerzas y reunión de los medios

La economía de fuerzas y reunión de los medios busca una adecuada distribución de las fuerzas con la finalidad de generar y lograr una superioridad relativa en

relación al enemigo (DD-10001 La Fuerza Terrestre, 2019). A primera vista, ello puede parecer menos aplicable, debido a la dispersión y distribución que se produce de la fuerza en pequeños núcleos.

Sin embargo, uno de los principales desafíos en la lucha contra la insurgencia es que se requiere una combinación de muchas capacidades para lograr el éxito. Si los medios militares desplegados (inteligencia, unidades de operaciones especiales, medios aéreos, etc.), y la fuerza policial no son utilizadas de manera efectiva, la insurgencia difícilmente podrá ser derrotada o al menos doblegada. Es decir, la economía y reunión de los medios al pretender la superioridad en los lugares donde se busca la decisión, permite éxitos parciales, los que en su conjunto, logran la victoria.

El mayor beneficio de la utilización de las fuerzas, no deriva en el actuar aislado de cada una de las unidades desplegadas en las distintas áreas de operaciones. Por el contrario, se deben aprovechar al máximo las capacidades de los medios puestos a disposición de un comandante para hacer frente a la insurgencia. Ello demanda que cada comandante piense en cómo va a emplear dichas unidades, dónde y cuándo sea requerido (reunión de los medios).

De ahí la importancia de operar con los medios disponibles y generar una fuerza capaz de trabajar de manera activa y coordinada; es decir, contar con un componente militar que esté en condiciones de cumplir diversas tareas con la menor cantidad de fuerza necesaria en las operaciones de configuración, a objeto de concentrar el poder de combate en la batalla decisiva (economía de las fuerzas). Uno de los ejemplos más notorios en este contexto, es el de las Fuerzas Armadas Israelitas. En la Operación “Escudo Defensivo” del año 2002[5], la adecuada combinación de inteligencia a través de la Agencia de Seguridad, la Inteligencia Militar y la Fuerza Aérea permitió identificar objetivos con gran

[5] Operación Militar Israelita, realizada entre el 29 de marzo y el 03 de mayo de 2002 durante el desarrollo de la segunda Intifada y cuyo objetivo principal era alcanzar infraestructura terrorista palestina y poner término a una serie de ataques terroristas contra los ciudadanos israelíes. Para mayor información, se sugiere revisar el siguiente link: https://www.idf.il/es/minisites/guerras-y-operaciones/operación-escudo-defensivo-2002/

precisión. Esta fue una acción militar que generó las condiciones adecuadas para concentrar el poder de combate a través de la reunión y economía de las fuerzas. Así, se evitó el daño colateral y se mantuvo el secreto y resguardo en la seguridad de las operaciones, permitiendo el éxito de las fuerzas en Judea, Samaria y la Franja de Gaza.

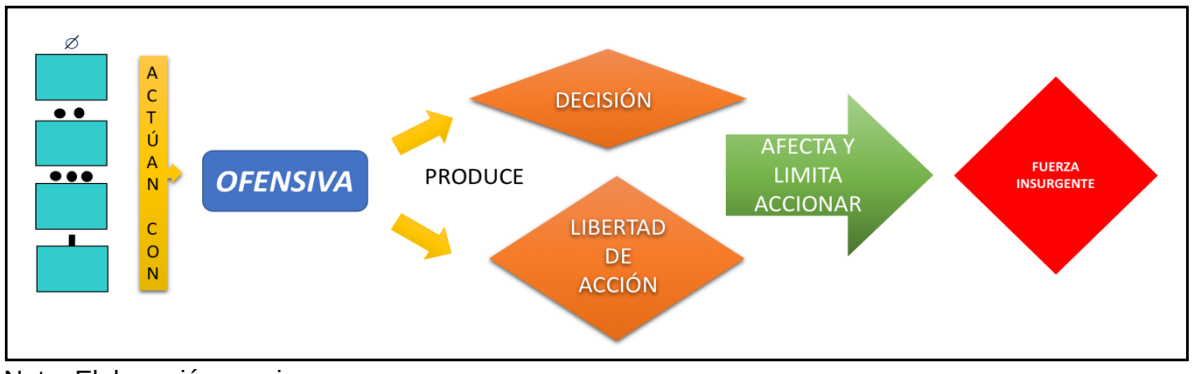
Como se aprecia, cada componente aporta con sus capacidades al proceso de estructuración de las fuerzas en el espacio de batalla. Dichas capacidades al ser combinadas, conducen a un resultado sinérgico, que es bastante más amplio en su objetivo final que el accionar de manera aislada o individual.

c. Ofensiva

El DD-10001 La Fuerza Terrestre (2019) asevera que la actitud ofensiva es el procedimiento más adecuado y efectivo para lograr la decisión y recuperar la libertad de acción. Este principio posee validez en todos los niveles de la conducción y tiene su mayor aplicabilidad en la lucha contra la insurgencia, ya que son los comandantes de las unidades subordinadas los que deberán tomar diversas resoluciones e iniciativas para poder hacer frente a esta amenaza.

Figura 5

Representación del principio de ofensiva



Nota. Elaboración propia.

Cada comandante debe comprender que el resultado de la ejecución de operaciones contra insurgentes, dependen de él y de las resoluciones provenientes del escalón superior. Lo anterior, entendiendo que, en principio, la

tarea en contra insurgencia es proteger a la población y, de forma secundaria, neutralizar a los grupos armados. Esa es la principal clave en el combate de pequeña unidad (escuadras y pelotones), característica propia de la forma en que se enfrenta al enemigo.

La ofensiva en contrainsurgencia puede darse a través de una fuerte campaña de informaciones, vinculada a una determinada acción social con la población o una fuerte campaña de deslegitimación de la fuerza insurgente, mediante hechos comprobatorios de la poca validez de su causa. Por ejemplo, lo ocurrido en la guerrilla colombiana y los asesinatos masivos de población rural.

Sin ser algo específico de la fuerza militar, una operación de información puede ejecutarse a través de diversos medios. No obstante, y a pesar de emplear recursos no militares, este tipo de operaciones deben estar bajo la supervisión u orientación de algún organismo de la defensa. De esta forma, se puede mantener la ofensiva de manera permanente, logrando conservar la libertad de acción y evitar que la fuerza insurgente la recupere o mantenga.

Finalmente, cada comandante debe tener clara la intención del escalón superior para accionar de manera ofensiva, generando con ello lo necesario para restablecer la iniciativa; lo que, sumado a los éxitos parciales, conllevan a la victoria.

d. Simplicidad

A pesar de que las operaciones de contrainsurgencia requieren de un gran nivel de detalle y coordinación en su planificación, ésta debe propender a ser tan simple como la “consecución del objetivo lo permita” (DD-10001 La Fuerza Terrestre, 2019, p. 170). Lo anterior, básicamente porque la insurgencia *per se* es compleja, debido a que la gran mayoría de las operaciones realizadas, se desarrollan entre la población civil. De ahí la importancia de este principio en el campo de batalla, el cual debe ser aplicado en todos los niveles de la conducción. Mientras más alto el nivel de la conducción, este principio cobra mayor relevancia, debido a que en los

eslabones más altos en la cadena de mando es donde se coordinan los distintos elementos del poder nacional para hacer frente a la insurgencia.

Sin este principio, serían pocas las operaciones que se ejecutarían por la falta del tiempo necesario para completar la preparación del proceso. Esto tiene mayor realce cuando se enfrenta a un enemigo esquivo y sin una cualidad específica que permita su identificación. Por tanto, la simplicidad permite tener una mayor facilidad en la interpretación y ejecución de las tareas que les son asignadas a las unidades con misiones de contrainsurgencia.

Es evidente que son los comandantes subordinados[6] quienes, debido a la segregación que se produce de las unidades, deben comprender de forma integral lo que se espera de ellos, logrando la simpleza en la ejecución de operaciones.

e. Unidad de esfuerzo

La unidad de esfuerzo significa asumir el conflicto bélico bajo una concepción de ideales, sacrificio y propósitos compartidos, que contribuyen a la protección o logro de los objetivos nacionales desde cualquier parte, buscando un efecto sinérgico en el accionar de las diferentes partes (DD-10001, La Fuerza Terrestre, p. 167).

En la lucha contra la insurgencia, el objetivo principal no es necesariamente un objetivo físico, sino más bien una actividad específica o un determinado individuo. Por lo tanto, la maniobra concebida para hacer frente a la insurgencia debe ser definida sobre qué es lo necesario para lograr los propios fines y evitar que la fuerza insurgente pueda cumplir sus objetivos. Los objetivos de la fuerza insurgente pasan a ser el centro de gravedad de la organización insurgente sobre el que hay que concentrar los esfuerzos buscando negar la posibilidad de alcanzarlo. Normalmente la insurgencia busca el apoyo de la población y centra su accionar sobre esta. En consecuencia, lo anterior se convierte en el criterio de ejecución, permitiendo definir la acción militar a realizar, lo que genera que la

[6] No actuando como brigadas o divisiones, sino que limitándose solo el empleo a unidades de magnitud de compañía y menores.

totalidad de los esfuerzos sean destinados y priorizados sobre un objetivo bien definido.

Figura 6

Representación del principio de la contrainsurgencia

Nota. Elaboración propia.

Las fuerzas armadas israelitas experimentaron la falta de este principio durante la Segunda Guerra del Líbano (2006), debido a que no concentraron y unificaron todos los esfuerzos en un determinado lugar y sobre un objetivo común para poder hacer frente a la amenaza irregular con la que se enfrentaban. Esto cambió cuando la misión fue definida como la destrucción o detención de cualquier cosa que permitiese el accionar de los grupos insurgentes tanto de los líderes de la organización de Hamas, como del técnico que ponía y preparaba los explosivos y/o aquellos individuos que colocaban o se inmolaban con dichos explosivos. Todos eran parte del objetivo. Una vez que esto fue definido, es cuando finalmente pudieron disminuir los índices de violencia en el área de operaciones.

Finalmente, lo que permite que el accionar de la contrainsurgencia contribuya al objetivo común es la sinergia que se produce entre todos los medios, mediante un esfuerzo coordinado y sincronizado, independiente de la manera en cómo se emplean.

f. Maniobra

Este principio tal como lo señala el DD-10001 La Fuerza Terrestre (2019), busca a través del movimiento de la fuerza posicionar al enemigo en una situación de desventaja, haciéndolo reaccionar de manera permanente a los estímulos de la propia fuerza hasta lograr su derrota. Es decir, pretende generar situaciones imprevistas que lo obliguen a resolver de manera acelerada y sin que su capacidad de alistamiento y reacción, le permitan hacer frente a situaciones de apremio.

En la contrainsurgencia el principio de maniobra debe buscar generar una continuidad en las acciones. Así, se logra producir desgaste en la insurgencia y crear las condiciones necesarias para mantener la libertad de acción, explotando las propias capacidades y atacando las vulnerabilidades adversarias. A esto se suma la dependencia de inteligencia, que no siempre es capaz de aclarar todas las dudas del comandante.

Este principio pasa a ser permanente en las acciones ejecutadas en todos los niveles de mando, por lo que la iniciativa en los comandantes subalternos adquiere gran relevancia en el actuar de la fuerza. Por tal razón, durante las operaciones se busca dejar al enemigo en un desbalance que puede ser transitorio de manera inicial; pero que, en la suma de acciones realizadas, permita generar la explotación del éxito para conseguir y alcanzar los objetivos propios mediante la maniobra.

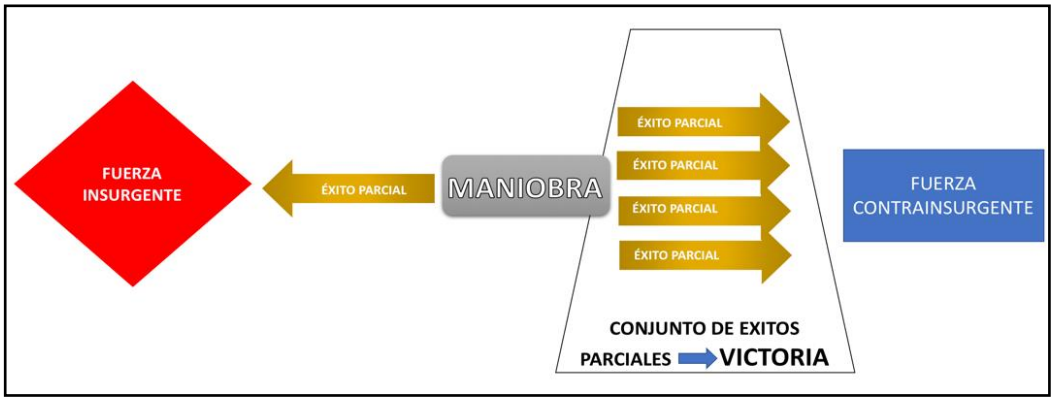
g. Libertad de acción

Debido a la configuración abstracta del ambiente operacional y a la manera en que el adversario desarrolla sus operaciones en la guerra irregular, se hace difícil poder identificar cuándo es posible aplicar este principio, ya que una vez iniciado el conflicto, la fuerza debe buscar obtener dicha libertad de acción y mantenerla. Por esta razón, la inteligencia cobra un valor relevante, debido a que contribuye a contar con la iniciativa en la ejecución de operaciones de contrainsurgencia.

A pesar de lo anterior, la libertad de acción es un principio que va cambiando tanto para el adversario como para la propia fuerza. Las diversas acciones que son desarrolladas no necesariamente van a contar con este principio de manera permanente, ya que muchas de ellas van a ser acciones de reacción, llevando la libertad de acción a momentos específicos en el contexto general de la operación.

Figura 7

El principio de libertad de acción en la contrainsurgencia



Nota. Elaboración propia.

Al ser un principio que tiene especial validez en la insurgencia, éste se debe tratar de lograr en los niveles más bajos, y a partir de esto, poder escalar para conseguirlo en lo operacional y estratégico. Es decir, pequeños éxitos tácticos que contribuyan a la libertad de acción a nivel operacional, generando con ello lo necesario para poder explotar al máximo las propias capacidades que permitan la libertad de acción necesaria en el desarrollo de las operaciones.

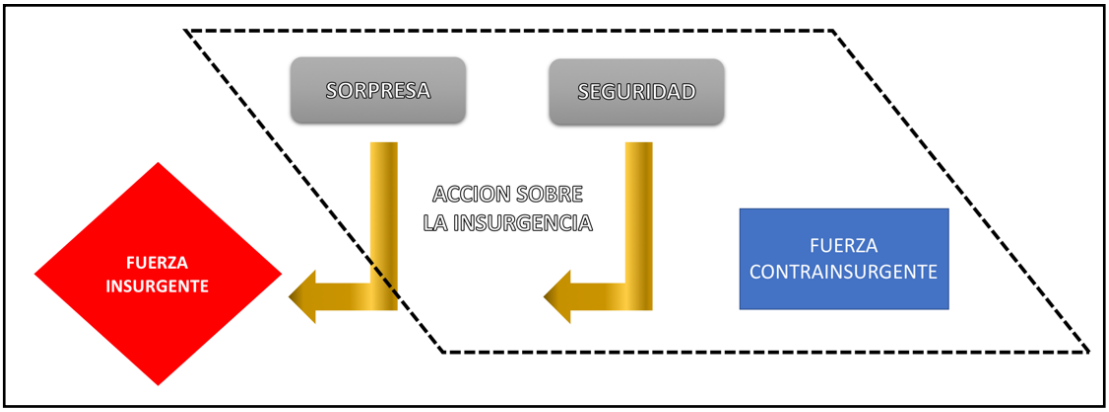
h. Sorpresa y seguridad

La sorpresa consiste en colocar al adversario en una situación para la cual no estaba preparado, permitiendo con ello, que sea incapaz de reaccionar (DD-10011 La Fuerza Terrestre, 2019). La sorpresa entonces, pasa a ser fundamental en la manera en que es ejecutada, ya que busca afectar al adversario insurgente y de esa manera, influir tanto de manera directa como indirecta, sobre su centro de gravedad.

La idea es generar la sorpresa en todos los niveles, y por eso su dificultad en poder aplicarla. Debe contar con inteligencia que permita generar las condiciones necesarias para actuar en el momento y lugar que se desea afectar, de acuerdo a lo que se sabe del adversario; y ser permanente en el empleo de las unidades ya que, en contraste con la guerra regular, donde la falta de sorpresa puede ser omitida con grandes fuerzas y poder de fuego, en la lucha contra la insurgencia lo señalado no es posible, ya que mucha fuerza aumenta la huella táctica y dificulta la relación con la población, pasando a constituir un problema que afecta a las operaciones.

Figura 8

El principio de sorpresa y seguridad



Nota. Elaboración propia.

Por otro lado, la seguridad es fundamental en todas las actividades desarrolladas contra la insurgencia, además de ser complemento de los principios de *maniobra y ofensiva*. Debido a su importancia, pasa a ser cuestionable el nivel de seguridad que se requiere para ejecutar las operaciones de contrainsurgencia. Esto porque se presentan variables en cuanto a la cantidad de fuerza que se emplea en las operaciones, así como la seguridad de la propia fuerza e incluso la seguridad de la población donde son desarrolladas las operaciones. De ahí la importancia que cada comandante evalúe cuál va a ser el nivel de seguridad que se le asigne a las

distintas operaciones desarrolladas, teniendo en cuenta los factores de análisis y la inteligencia (factor fundamental en el despliegue de las unidades).

Finalmente, el nivel de seguridad con que se cuenta en una determinada área de operaciones está definida en muchos casos por la ausencia de violencia física, el mantenimiento del respeto a las leyes, la protección de los derechos humanos y la libertad para realizar actividades de desarrollo social. Producto de lo anterior, se debe asumir el contar con la mayor cantidad de certeza posible, sin que esto pase a ser un exceso, tanto en los procesos previos como en el riesgo que se esté dispuesto a asumir. En consecuencia, las capacidades e información que se tenga del adversario, adquieren especial significado en la manera en que es ejecutada la seguridad de las operaciones en la contrainsurgencia.

i. Unidad de mando

Tal como lo indica su nombre, la unidad de mando se refiere a que un sólo comandante dirige y coordina las acciones de la totalidad de la fuerza hacia un objetivo común (DD-10011 La Fuerza Terrestre, 2019). Debido a la naturaleza interagencial, propia del desarrollo de las operaciones de contrainsurgencia, se generan situaciones donde el comandante no siempre mantiene el control de la totalidad de los medios que se desempeñan en una determinada área de operaciones. A pesar de esto, los comandantes en todos los niveles deben propender a generar, mediante el diálogo y la adecuada coordinación, la unidad de esfuerzo necesaria que permita de manera indirecta la unidad de mando entre los medios militares y no militares.

Como son diversos los medios que actúan en la lucha contra la insurgencia, el que exista solo un mando que dirija la totalidad de la fuerza, en pos de un objetivo común, va a permitir la obtención de mejores resultados. Esto se traduce en que la totalidad de los mandos, independiente del nivel en el que se desempeñen, así como las fuerzas y medios participantes en la contrainsurgencia, deban estar alineados en los objetivos planteados, permitiendo la continuidad en el desarrollo de las operaciones. La unidad de mando es un principio complejo de aplicar en las

operaciones de contrainsurgencia, pero teniendo conciencia de su relevancia, se puede establecer una adecuada coordinación entre los medios y recursos involucrados, facilitando con ello la adecuada aplicación del principio.

REFLEXIONES FINALES

Los principios de la guerra tienen plena validez y pueden ser aplicados por los comandantes y sus estados mayores o planas mayores de todos los niveles en la lucha contra la insurgencia; sin embargo, es importante considerar que en el proceso de análisis difiere considerablemente en cómo son utilizados y empleados por un comandante, su estado mayor o plana mayor, en el contexto de la guerra regular. Esto debido a que una de las grandes diferencias entre lo que se conoce como guerra regular e irregular, de acuerdo a lo analizado en el artículo, es que esta última involucra a objetivos relevantes con la disputa por el apoyo de la población civil, siendo este factor el que condiciona y, a la vez, dificulta el utilizar los principios de la guerra en el proceso de análisis y posterior toma de decisiones.

Es el comandante el que prioriza y evalúa cómo adaptarlos en la estructuración de su maniobra. Excepto por el principio de “definición y mantención del objetivo”, todo el resto depende únicamente del comandante y en cómo aprecia y analiza la situación en la que se ve envuelto (problema militar), lo que determina su aplicación.

Asimismo, existe una dificultad permanente relacionada con la exposición a los medios de comunicación social, donde los comandantes y las decisiones que estos adoptan son expuestas en tiempo real. Por tanto, se requiere que las operaciones de contrainsurgencia sean acompañadas de una fuerte campaña de INFOOPS, lo que obliga y condiciona muchas veces el empleo de la fuerza y, por ende, el poder aplicar los principios de la guerra.

Otro aspecto a tener en cuenta es que la lucha contra la insurgencia y la complejidad que ésta presenta, va vinculada a poder generar la sinergia necesaria entre la inteligencia que se recibe y la acción a ejecutar. Coordinar y sincronizar el actuar de las fuerzas (desde pequeña unidad hasta Unidades de Armas

Combinadas), sumado a la dificultad propia de la totalidad de las operaciones (las que son desarrolladas en una población mixta, de insurgentes y civiles) complejiza el desarrollo de las operaciones, ya que se debe buscar la manera de aislar a los insurgentes de los civiles, logrando con ello que la acción militar sea legitimada.

Finalmente, cada uno de los principios analizados en este artículo, tomados de manera individual o en conjunto, constituyen una guía para los comandantes y asesores al enfrentar este tipo de conflicto. Para esto, es pertinente tener presente su especial naturaleza y filosofía, además del contexto histórico en el que se desarrollan, por lo tanto, se estima que tienen plena validez al ser aplicados en la lucha contra la insurgencia.

REFERENCIAS

Amidror, Y. (2010). Winning Counterinsurgency war: The Israeli Experience. *Strategic Perspectives Nº2.* https://jcpa.org/wp-content/uploads/2011/11/Amidror-perspectives-2.pdf

Arreguin-Toft, I. (2001). How the weak win wars: A Theory of Asymmetric Conflict. *International Security,* 26(1), 93-128. https://web.stanford.edu/class/polisci211z/2.2/Arreguin-Toft%20IS%202001.pdf

Cepeda, L. (2016). Teoría de la Guerra de Clausewitz en la lucha contra la Insurgencia (COIN): ¿Mantiene su validez? Revista *del Instituto Español de Estudios Estratégicos (IEEE)*, (7), 59-87. https://revista.ieee.es/article/view/232/388

De Benedetti, D. (2013). *Insurgencia y contrainsurgencia en los inicios del nuevo siglo.* X Jornadas de Sociología. Facultad de Ciencias Sociales, Universidad de Buenos Aires.

Ejército de Chile, División Doctrina. (2019). *DD 10001 La Fuerza Terrestre*.

Ejército de Chile, División Doctrina. (2017). *DD 10001 El Ejército.*

Ejército de Chile, División Doctrina. (2012). *RDO 20001 Operaciones*.

Ettrich, B. (2005). *The Principles of War: Are they still applicable?* Naval Postgraduate School. https://apps.dtic.mil/dtic/tr/fulltext/u2/a435689.pdf

Gallardo, M (2020). *¿Cómo definir el pensamiento estratégico?* Centro de Estudios Estrategicos de la Academia de Guerra (1). https://www.ceeag.cl/wp-content/uploads/2020/05/Pensamiento.pdf

Harrelson, L. (2005). *The Principles of War: Valid Yesterday, Today and Tomorrow*. Joint Forces Staff College. https://apps.dtic.mil/dtic/tr/fulltext/u2/a436747.pdf

Joint Publication 3-24. (2018). *JP 3-24 Counterinsurgency.* Washington DC. Doctrine Publications.

Lauriani, C. (2019). Operaciones militares en la provincia de Ambar, el punto de inflexión de la estrategia de contrainsurgencia en la Guerra de Irak. *Memorial del Ejército de Chile*. Centro de Estudios e Investigaciones Militares, (504), 127-136.

Lindemann, M. (2010). Laboratorio de Asimetría: La guerra del Líbano de 2006 y la Evolución de las Tácticas Terrestres Iraníes. *Military Review*, (Julio-Agosto), 77-88. https://www.armyupress.army.mil/Portals/7/military-review/Archives/Spanish/MilitaryReview_20100831_art011SPA.pdf

Operación Escudo Defensivo. (2002). *Israel.* Fuerzas de Defensa Israelí. https://www.idf.il/es/minisites/guerras-y-operaciones/operación-escudo-defensivo-2002/

Reed, T., y Donahoe, A. (2004). *The Tao of Special Forces: An Analysis of Counterinsurgency Doctrine*. Naval Postgraduate School. https://calhoun.nps.edu/handle/10945/1597

Sanchez, P., y Rodríguez, J. (2008). El Conflicto del Libano. *Conflictos internacionales Contemporáneos (11)*. Ministerio de Defensa Español.

United States of America, Department of the Army. (2014). *Field Manual. FM 3-24 MCWP 3-33.5* Insurgencies and Countering Insurgencies. https://fas.org/irp/doddir/army/fm3-24.pdf

US Government. (2012). *Guide to the Analysis of Insurgency*. US Government publications. https://www.hsdl .org/?abstract&did=713599

US Government. (2009). *Counterinsurgency Guide.* US Government publications. https://2009-2017.state.gov/documents/organization/119629.pdf

United States of America, Department of Defense. (2007). *Irregular Warfare (IW) Joint Operational Concept (JOC)*. Version 1.0. https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joc_iw_v1.pdf?ver=2017-12-28-162020-260

Van Avery, C. (2007). *12 New principles of War*. Armed Forces Journal. http://armedforcesjournal.com/12-new-principles-of-warfare

DESAFÍOS DE LA TECNOLOGÍA 5G EN EL ÁMBITO DE LA CIBERSEGURIDAD

Challenges of 5G technology in the field of cybersecurity

MAY. Juan Pablo Nieny Hodar*

Resumen: En plena *Cuarta Revolución Industrial* (4RI), la tecnología avanza a una velocidad que supera la capacidad de los estados para adaptarse. En ese sentido, la implementación de la tecnología 5G en Chile, prevista para inicios del 2022, presenta amplias oportunidades para muchas áreas, como el teletrabajo, la telemedicina, la modernización del Estado, el desarrollo de capacidades estratégicas, las ciudades inteligentes, el aumento de la productividad, el internet de las cosas (IoT), el e-commerce, entre otras; sin embargo, los desafíos son insospechados. Por consiguiente, los estados no solo deben asumir que existirán riesgos, sino también potenciales problemas de seguridad. El presente artículo revisarán los desafíos que se generan a partir de la implementación de la tecnología 5G en el ámbito de la ciberseguridad.

Palabras claves: 5G, ciberseguridad, desafíos

Abstract: In the midst of the *Fourth Industrial Revolution* (4IR), technology is advancing at a speed that exceeds the ability of states to adapt. Accordingly, the implementation of 5G technology in Chile, scheduled for early 2022, presents opportunities for many areas, such as teleworking, telemedicine, modernization of the State, the development of strategic capacities, smart cities, increased productivity, the internet of things (IoT) and e-commerce, among others. However, these opportunities present unsuspected challenges. Therefore, States must not only assume that there will be risks, but also challenges to national security. The article will revise these security challenges arising from the implementation of 5G technology in the area of cybersecurity.

* Oficial del Arma de Caballería Blindada. Magíster en Ciencias Militares con mención en Gestión Estratégica. Actualmente es alumno del Tercer año del Curso Regular de Estado Mayor en la Academia de Guerra del Ejército de Chile. ✉juan.nieny@acague.cl

***Key words**:* 5G, cybersecurity, challenges

INTRODUCCIÓN

La comunicación ha sido una de las características centrales de la sociedad, desde el hombre primigenio hasta nuestros días. Niklas Luhmann, sociólogo alemán, explica en su teoría general de sistemas que la comunicación permite que el *sistema social*[1] trascienda y se perpetúe (Luhmann, 2012). En otras palabras, la sociedad es un sistema de comunicaciones per se. Dado lo anterior, la comunicación cobra aún mayor valor en medio de la era de la Información.

El fenómeno de la *Cuarta Revolución Industrial* (4RI), que habría comenzado a inicios del siglo XXI, ha generado cambios profundos en todos los sectores de la sociedad y ha permitido un elevado desarrollo de aquellas herramientas vinculadas a la transmisión, procesamiento y almacenamiento de datos digitales. Es así como la informática se ha visto sometida a una evolución que pareciera no tener límites, configurando un mundo híper-conectado.

Por otra parte, Klaus Schwab indica que la 4RI tendrá un profundo impacto en la naturaleza de las relaciones internacionales y dedica especial atención a ello en su obra:

> De todas las transformaciones importantes vinculadas a la cuarta revolución industrial, la seguridad es una [cuestión][2] insuficientemente discutida en el dominio público y en los sectores fuera de los gobiernos y la industria de la defensa. (Schwab, 2016, p. 67)

En ese orden de ideas, la implementación de la tecnología 5G en Chile se transforma en un desafío para el Estado, ya que existen una serie de riesgos asociados a esta nueva generación de comunicaciones inalámbricas. Diversos medios coinciden en señalar que la tecnología 5G permitirá aumentar diez veces la velocidad de navegación en internet. Además, disminuirá drásticamente la tasa

[1] Niklas Luhmann considera tres sistemas en su teoría general de sistemas: el sistema vivo, el sistema psíquico y el sistema social.

[2] Palabra sugerida por el autor, debido a que el texto original no la contiene.

de latencia[3], lo que se traducirá en la posibilidad de incrementar dispositivos conectados a una red, facilitando el denominado el *internet de las cosas* o *internet of things* (IoT), como lo fue en su momento el internet móvil para la tecnología 4G.

Al mismo tiempo, países como Estados Unidos, Inglaterra, entre otros, han alertado al mundo sobre los riesgos que supone que ciertos proveedores participen en la implementación de infraestructura y servicios asociados a la tecnología 5G, principalmente por riesgos a la seguridad por acciones como espionaje, vigilancia cibernética y apagones informáticos (BBC, 2020). Por otra parte, las ventajas del 5G abren también la posibilidad a las ciberamenazas, las que ponen el foco en el robo de datos, ciberataques y otras actividades de cibercrimen.

En consecuencia, con un horizonte proyectado al 2022 para la implementación del 5G en el país y considerando que ya se han adoptado medidas concretas al respecto, conviene revisar las implicancias de la adopción de esta nueva generación de conectividad inalámbrica para gestionar, conectar y organizar el propio Estado.

Al respecto, el presente artículo busca responder a la interrogante ¿Cuáles son los desafíos de la tecnología 5G en el ámbito de la Ciberseguridad? Para abordarla, inicialmente se contextualiza en relación a la 4RI y a la aceleración tecnológica; posteriormente, se entregan algunos detalles técnicos sobre el 5G, sus ventajas y beneficios; seguidamente, se reflexiona sobre los riesgos asociados a esta nueva tecnología; y, finalmente, se exponen algunos desafíos vinculados a la adopción del 5G. Lo anterior, considerando un contexto, que busca transformar a algunos estados en países ciber-resilientes[4].

---

[3] La latencia es el tiempo que demora en transmitirse un paquete de datos en una red. Corresponde a una unidad de medida de tiempo, expresada en milisegundos. No debe confundirse con la velocidad de conexión que dice relación con la cantidad de información enviada y/o recibida.

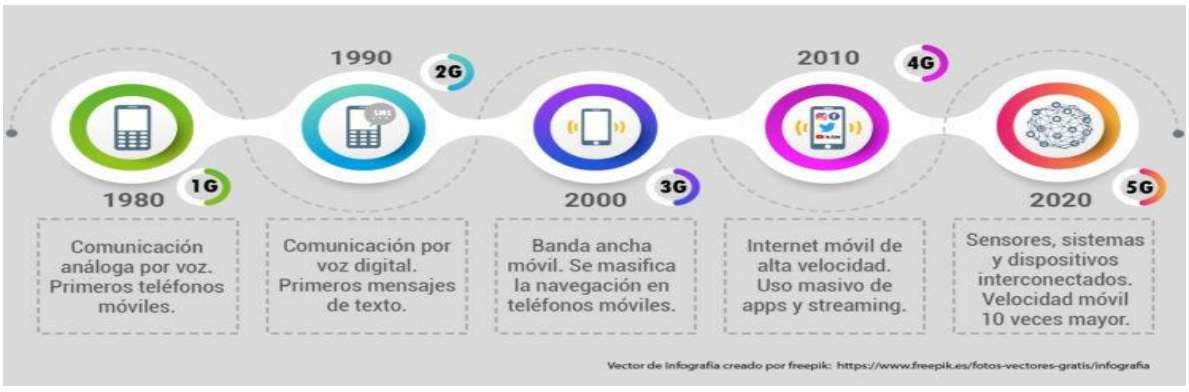
[4] Existen múltiples definiciones para el concepto de ciber-resiliencia (cyber resiliency o cyber resilience). La organización norteamericana The MITRE Corporation, por ejemplo, la define como la capacidad de anticipar, resistir, recuperarse de, y adaptarse a condiciones adversas, estrés, ataques o compromisos en los recursos cibernéticos. Asimismo, el Instituto Nacional de

LA CUARTA REVOLUCIÓN INDUSTRIAL Y EL ACELERADO DESARROLLO TECNOLÓGICO

Es comentado que el mundo actualmente se encuentra experimentando la cuarta revolución industrial, en la que existe un desarrollo exponencial de la tecnología. Según Klaus Schwab, fundador del Foro Económico Mundial y autor del libro *La Cuarta Revolución Industrial*, esta "...se basa en la revolución digital. Se caracteriza por un internet más ubicuo y móvil, por sensores más pequeños y potentes que son cada vez más baratos, y por la inteligencia artificial y el aprendizaje de la máquina" (Schwab, 2016, p. 14). En este contexto se enmarcan las redes de comunicaciones de quinta generación o 5G, tecnología que permitirá incrementar ostensiblemente la velocidad de conexión inalámbrica entre aparatos y desde estos hacia la red Internet. En lo referido a la industria de telefonía móvil, desde la aparición del celular con tecnología de primera generación (1G), la aceleración tecnológica, casualidad o no, ha permitido la renovación generacional cada 10 años (Ver Figura 1). Es dable esperar, por lo tanto, que antes del 2030 ya se esté hablando de la sexta generación (6G).

Figura 1

Evolución de las generaciones de telefonía celular



Nota. Adaptado de Juan Carlos Mena, "Ventajas, desventajas y mitos de la tecnología 5G" (https://www.uao.edu.co/ingenieria/ventajas-desventajas-y-mitos-de-la-tecnologia-5g/).

Ciberseguridad Español (INCIBE) hace referencia a la capacidad para resistir, proteger y defender el uso del ciberespacio de los atacantes.

¿QUÉ ES EL 5G?

La tecnología 5G corresponde a la quinta generación de tecnología de comunicaciones inalámbrica para celulares, por tanto es la más avanzada tecnología de redes de datos. Técnicamente, se señala que la experiencia de navegación de un usuario promedio de internet, aumentará 10 veces o más en comparación a las actuales redes de datos 4G. Pero no solo eso, la nueva tecnología permitirá aumentar ostensiblemente la cantidad de aparatos que se conectan a una determinada red y la interacción entre ellos, permitiendo un salto significativo para el denominado *internet de las cosas* (IoT) y para la comunicación máquina a máquina (M2M), ampliando la gama de nuevos usos y produciendo un gran impacto sobre la forma en que vivimos.

En los próximos años, el mundo será testigo de cómo se conectan y controlan remotamente una infinidad de dispositivos (robots, drones, servidores, automóviles, tablets, smartphones, electrodomésticos, cámaras de vigilancia, etc.), con múltiples propósitos como la telemedicina, el teletrabajo, el control productivo, la conducción autónoma, el cloud computing, el big data, el entretenimiento, entre otros. Así, las ciudades deberán migrar hacia el concepto de ciudad inteligente o *smart city*, como una evolución del concepto de ciudad digital.

Dado que el 5G utiliza ondas de frecuencia más altas que las redes 4G y que estas ondas recorren menos distancia, consecuentemente, una de las caraterísticas de las smart cities será la proliferación de antenas que permitan el acceso ininterrumpido de los dispositivos (ver desventajas en Cuadro 1). Considerando estas y otras características “las antenas 5G serán un nuevo tipo de antenas que estarán altamente integradas, admitirán una configuración flexible de todas las bandas y permitirán la gestión de haces en situaciones específicas”[5] (Huawei, 2019, p. 7).

[5] Traducción del autor.

Si bien en el año 2008 se creó un proyecto surcoreano llamado *5G mobile communication systems based on beam-division multiple access and relays with group cooperation*, según la 3GPP[6] la quinta generación de redes móviles nace el año 2018 de manera oficial. En comparación a su predecesora, la tecnología 5G presenta ventajas y desventajas que conviene resaltar:

Cuadro 1

Ventajas y desventajas de la tecnología 5G

Ventajas	Desventajas
Aumento de la velocidad de usuario en 10 veces. Es decir, si la tecnología 4G contaba con 10 MB/sec (Megabit por segundo), la 5G aumenta hasta 100 MB/sec.	El 5G al utilizar frecuencias de radio más altas, tendrá un rango de cobertura menor. Por tanto, los operadores necesitarán instalar más nodos (antenas) en el país, lo que tomará más tiempo para dar cobertura total.
Mayor movilidad. El 4G había definido velocidades hasta de 300 km/h, a velocidades mayores ya no cumplía el estándar. 5G aplica incluso para velocidades de hasta 500 km/h, esto significa que con esta red se podrá tener buena comunicación incluso en aeronaves.	Requiere de nueva infraestructura (CW), nuevos equipos de radio (NR) donde integra las 3 tecnologías de radio (RAT 2G, 3G y 4G), con mayor potencia con las nuevas bandas de operación de 5G.
Menor latencia. En 4G teníamos latencias de hasta 10 milisegundos, en 5G de hasta un milisegundo. Las áreas más beneficiadas serán la de los carros autónomos y la salud.	Usuarios deberán adquirir nuevos equipos como teléfonos, tabletas, computadores, etc.
Densidad de conexión mayor. En 4G era una densidad por km^2 de hasta 100 mil dispositivos, en 5G podremos tener hasta un millón de conexiones por km^2.	

[6] Organización que reúne a un grupo de asociaciones de telecomunicaciones de distintas partes del mundo con el propósito de definir especificaciones y estándares para la industria de la telefonía celular.

Mayor eficiencia energética de la red. Las antenas van a consumir menos potencia, lo que genera un ahorro de energía de hasta 100 veces en una estación base. Las baterías de los celulares tendrán una eficiencia de energía de hasta 100 veces más que la actual.	
La capacidad de tráfico por área será de 10 MB/sec x m^2, mientras en 4G no alcanzaba ni a los 0.1 MB.	
Se tendrán velocidades de hasta 20 GB/sec.	

Nota. Adaptado de Juan Carlos Mena, "Ventajas, desventajas y mitos de la tecnología 5G" (https://www.uao.edu.co/ingenieria/ventajas-desventajas-y-mitos-de-la-tecnologia-5g/).

NUEVAS TECNOLOGÍAS, NUEVO ENTORNO

En Chile y en diversos países de la región, existe un gran entusiasmo respecto de los avances tecnológicos y lo que ofrece la tecnología 5G. Sin embargo, en el ámbito de la tecnología y de la información, existe preocupación por los riesgos que ella podría presentar para la seguridad. Y esto como resultado de una simple lógica: a mayor conectividad, mayores puntos de acceso y oportunidades para explotar de manera maliciosa las vulnerabilidades de las redes. Si tomamos en cuenta que la tecnología 5G expandirá el uso del IoT, los riesgos a la seguridad aumentarán enormemente.

Grandes potencias ya lo han advertido y las preocupaciones por espionaje o interrupción de comunicaciones son las razones aducidas.

A lo anterior, se podrían agregar otros factores. Y es que el 5G no solo supone el aumento de riesgos de robo de información digital, espionaje o apagones, sino que también de daño masivo a infraestructura. Esto debido a que en un mundo hiperconectado, muchos procesos serán controlados y dependerán de redes informáticas para su funcionamiento.

Como comentan Purdy, Yordanov y Kler, el año 2013 la empresa Target, una de las cadenas de retail más importantes de Estados Unidos, sufrió un ciberataque que le costó US$292 millones solamente en compensaciones legales, sin contar

costos de ventas y otros perjuicios. El ataque se produjo a través de un proveedor de servicios de climatización que tenía autorización para acceder a sus servidores y monitorear remotamente la temperatura y consumo de energía de sus tiendas (Purdy et al., 2020, p. 117).

Una experiencia de esas características, supondría el fin de muchas empresas, por la incapacidad de soportar los perjuicios. El artículo, titulado *Don't Trust Anyone,* sugiere que las posibilidades de sufrir un ataque se diversifican con la tecnología 5G, y es categórico en señalar que no se puede confiar en nadie. Además, plantea que mientras algunos adversarios de Estados Unidos estarían desarrollando capacidades para apagar remotamente las redes inalámbricas, otros, podrían utilizar sus capacidades submarinas para, literalmente "cortar los cables" de las redes 5G (Purdy et al., 2020, p. 119). Estas ideas dan cuenta de los daños potenciales y los efectos que podrían tener sobre los gobiernos, empresas, industrias y público en general.

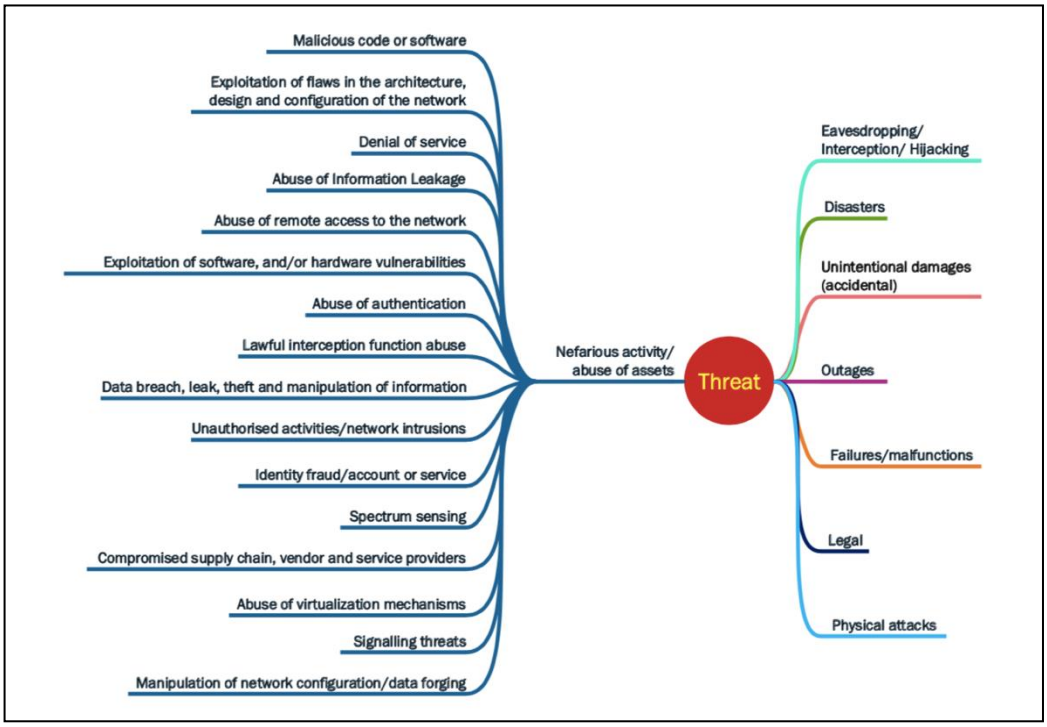
Por lo anterior y un cúmulo de otros ejemplos, se evidenciaría que IoT continuará siendo un desafío y foco de amenazas para la red 5G, sobretodo porque la mayoría de los dispositivos que podrán interconectarse a redes inalámbricas 5G.

Por otra parte, la Unión Europea también ha abordado la problemática de la seguridad de las redes 5G. La Agencia de la Unión Europea para la Ciberseguridad (ENISA), publicó en noviembre de 2019 un reporte titulado *ENISA Threat Landscape For 5G Networks*[7]*.* En el documento, se busca identificar aquellos componentes más críticos de las redes 5G y que pueden quedar expuestos a las ciberamenazas. Además presenta una interesante taxonomía de amenazas para las redes 5G (ver Figura 2). Coincidiendo con muchas voces expertas en relación con esta tecnología, señala que "los riesgos y amenazas aún no se han entendido por completo" (ENISA, 2019, p. 54).

[7] El reporte *ENISA Threat Landscape For 5G Networks,* puede ser consultado en https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks

Figura 2

Taxonomía de amenazas según ENISA



Nota. European Union Agency for Cibersecurity, (2019), “ENISA Threat Landscape For 5G Networks”, p. 64.

La reflexión que se hace es coincidente con el planteamiento del fundador del Foro Económico Mundial sobre la 4RI respecto a que “tenemos solo una comprensión limitada del máximo potencial de la nuevas tecnologías y de lo que vendrá en el futuro” (Schwab, 2016, p. 71). Estas ideas refuerzan la premisa de que la ciberseguridad debe ser un imperativo para los Estados.

Las 58 amenazas que detalla el reporte, además de las 8 categorías de agentes responsables de las ciberamenazas (cibercriminales, actores internos o insiders, Estados-Naciones, ciberguerreros, hacktivistas, corporaciones, ciberterroristas y script kiddies) permiten comprender lo vulnerable que será la sociedad internacional para cuando la tecnología 5G esté completamente implementada.

En 2003, Kirk Bailey, jefe de la oficina de seguridad de la información de la Universidad de Washington, introducía el concepto de *asumir la brecha* en materias de ciberseguridad (citado por Purdy et al., 2020, p. 122). Con los

actuales avances en tecnología y los que llegarán en el mediano plazo de la mano del 5G, un ataque informático ya no debe abordarse en términos de una posibilidad, sino que de una certeza, quedando solo pendiente conocer "cuándo" este ocurrirá. Esta filosofía ha ayudado a todos los sectores a estar más preparados para las ciberamenazas. Lo anterior nos advierte sobre el cambio en los paradigmas de ciberseguridad hacia la aceptación de vulnerabilidades.

Pero ¿Qué pueden hacer los estados al respecto? Ciertamente, existe mucho entusiasmo de los gobiernos para no quedar atrás en la implementación del 5G. El caso chileno ha sido destacado por la hoja de ruta que ha sido trazada sobre la materia. Evidencias de ello son el plan de Matriz Digital 2018-2022, la Agenda Digital, la difusión durante el año pasado del lanzamiento de la primera licitación nacional para redes 5G, el impulso de carreteras digitales a través de fibra óptica para sectores aislados del país, la firma de diversos memorándum de entendimiento (MoU) con países como España, Israel, Colombia, Ecuador, Reino Unido y Estonia, entre otras iniciativas orientadas al aprovechamiento de las oportunidades que ofrece el mejoramiento de las redes inalámbricas.

No obstante ¿Qué hay en materia de ciberseguridad? De acuerdo con el reporte del Foro Económico Mundial, *The Global Risks Report 2021*[8]*,* publicado en enero del presente año, los riesgos de tipo tecnológico (fraude o robo de datos y ciberataques) han ocupado entre el 2do y 3er lugar en el ranking de los mayores riesgos globales en términos de probabilidad de ocurrencia en los cuatro últimos años (2018, 2019, 2020 y 2021), después de los riesgos del medio ambiente los tres primeros años y en 2021 por detrás de los riesgos sociales que implican las enfermedades infecciosas (WEF, 2021).

Chile, a pesar de los avances logrados en materias de telecomunicaciones y a diferencia de lo que normalmente piensa el común de las personas, estaría igualmente expuesto. Y es que mayor desarrollo no implica necesariamente mayor seguridad.

[8] El reporte *The Global Risks Report 2021* y otras versiones anteriores, puede ser consultado en https://www.weforum.org/reports.

Según Eduardo Parada, Gerente de Ingeniería de la Consultora TI Vector, en entrevista realizada por el portal de noticias Emol.com (2017), "el país ocupa el quinto lugar latinoamericano con más usuarios afectados por ciberataques, con un 20,6%, por detrás de Brasil (30%), Honduras (23,5%), Panamá (22,6%) y Guatemala (21,6%)".

Por otra parte, el sitio *Threat Intelligence Insider Latin America* de Fortinet, señala que Chile fue objeto de 525 millones de intentos de ciberataques durante la primera mitad del año 2020 (RoiPress, 2020). El sitio advierte que en el contexto de la pandemia por COVID-19, los ataques han aumentado y han incrementado el grado de sofisticación, tendencia que podría mantenerse durante los próximos años (Fortinet, 2020).

Contrario a los datos expuestos, y a modo de contrargumento, se podría sostener que Chile es un país ciber seguro y que los datos utilizados en la mayoría de los reportes apuntan a empresas civiles y no a entidades de gobierno. De igual manera, es conveniente recordar que ciertas entidades públicas también han sido objeto de ciberataques, lo que da cuenta de estándares de ciberseguridad similares para el sector público y el privado. Evidencia de lo anterior, son los ciberataques sufridos por Banco Estado durante junio y septiembre del 2020, siendo el último de ellos presumiblemente provocado por hackers (La Nación, 2020). Además, se infiere que la mayoría de las motivaciones para llevar a cabo los ciberataques a empresas privadas y/o instituciones financieras, obedecen a motivaciones criminales para la obtención de dinero, lo cual durante la pandemia y de acuerdo a diversos medios se ha ido incrementando. Sin embargo, si las motivaciones fueran políticas, estos buscarían sitios o infraestructura del Estado.

Y es que el dominio del ciberespacio[9] ofrece una serie de beneficios a la hora de enfrentar a las nuevas amenazas[10] y lograr la iniciativa en la *guerra de la*

[9] Existe consenso entre las fuerzas armadas del mundo en distinguir 5 dominios en el ambiente operacional: el terrestre, el naval, el aéreo, el espacial y el ciberespacio.

[10] Existen diversas conceptualizaciones sobre nuevas amenazas o amenazas emergentes en la literatura. La OEA, por ejemplo, en el año 2003, en la Declaración sobre Seguridad en las Américas, planteaba un enfoque de Seguridad Multidimensional y calificaba como nuevas amenazas al terrorismo, la delincuencia organizada transnacional, la narcoactividad, el tráfico

información (information warfare/IW)[11]. Así lo han entendido las principales potencias mundiales. Estados Unidos, por ejemplo, creó en 2008 el U.S Cyber Command (USCYBERCOM), unidad de comando de nivel estratégico que entró en pleno funcionamiento el 2010, con la responsabilidad de planificar y conducir operaciones militares en el ciberespacio. China, en 1995 iniciaba un plan de IW y en 2000 establecía una unidad estratégica de IW (Ball, 2011).

Si pensamos en la fuerte dependencia que tendrá (o que ya tiene) la sociedad hacia las TICs a propósito de la implementación de la tecnología 5G y, observando las capacidades informáticas que tienen (y que tendrán) las grandes potencias y las relaciones de poder entre ellas, la mayoría ligadas a las principales empresas proveedoras de servicios 5G, entonces no es arriesgado pensar que se pueda generar una suerte de *influencia indirecta* de estados de mayor estatura estratégica hacia los más pequeños, como lo expresa el Coronel el Ejército Español Pedro Baños en su texto orientado a analizar las que considera claves del poder mundial (Baños, 2017, p. 165). Aspectos cualitativos como éstos en el ámbito de las relaciones internacionales, alejados del tecnicismo propio de la tecnología, deberían ser incluidos en los análisis multifactoriales para adoptar definiciones y decisiones sobre la materia.

Ahora bien ¿Qué dicen los indicadores y referencias internacionales respecto de Chile en materia de ciberseguridad? De acuerdo a lo que señala el *National Cyber Security Index*[12], que mide las capacidades de ciberseguridad implementadas por los gobiernos, Chile actualmente ocupa el lugar 39 de un total de 160 países evaluados (NCSI, 2020). En el plano regional, solo Paraguay (nº 38) superó a Chile a partir de la medición de 2020. El resto de los países sudamericanos se ubican en puestos inferiores (entre el 57 y 95).

ilícito de armas, el lavado de activos, los desastres naturales, los desastres de origen antrópico, la trata de personas, los ataques a la seguridad cibernética, entre otros.

[11] Según el académico Milán Vego, reconocido por sus estudios sobre el arte operacional, la guerra de la información corresponde a todas aquellas acciones destinadas a lograr la superioridad de la información negando, explotando, corrompiendo o destruyendo la del enemigo mientras se protege la información y las funciones propias del ataque enemigo.

[12] El ranking del National Cyber Security Index puede ser consultado en https://ncsi.ega.ee/ncsi-index/

A nivel global, destaca Estonia (nº 3), país que el año 2007 sufrió un ciberataque contra organismos estatales e instituciones financieras presumiblemente por parte de hackers rusos. Las consecuencias fueron nefastas generándose una paralización digital del país por semanas (BBC, 2017). Estonia, a la fuerza, aprendió la lección y hoy es un referente en materias de Ciberseguridad y Ciberdefensa. Claramente ningún Estado quiere aprender de esa manera; por ello, se debe sensibilizar a la población y, particularmente, a las autoridades en materias de ciberseguridad, asumiendo por cierto las debilidades del Estado y adoptándose un paradigma de ciber-resiliencia a nivel país.

Otro índice global que conviene observar, es el *Global Cybersecurity Index*, una iniciativa de la International Telecommunication Union (ITU) que ofrece una referencia global para los países en materias de ciberseguridad. El Índice de Ciberseguridad Global (GCI) es un "índice compuesto que combina 25 indicadores en un punto de referencia para monitorear y comparar el nivel de compromiso de ciberseguridad de los países con respecto a los cinco pilares de la Agenda de Ciberseguridad Global (GCA)" (ITU, 2018), detalla el último reporte GCI del año 2018[13]. Chile aparece en el puesto nº 83 a nivel global y nº 9 en América; por debajo de Estados Unidos, Canadá, Uruguay, México, Paraguay, Brasil, Colombia y Cuba, dos puestos más abajo que en el GCI 2014. Al respecto, Carlos Landeros, Director Nacional del CSIRT[14], señalaba en julio de 2019, que la posición de Chile debiera mejorar en las próximas mediciones puesto que se han logrado una serie de avances sustanciales en los últimos años (MININT, 2019). Cabe resaltar que existe una correlación entre los cinco pilares[15] de la GCA y los cinco ejes estratégicos definidos por la Política Nacional de Ciberseguridad 2017-2022: Infraestructura, Legislación, Difusión, Colaboración Internacional y Desarrollo de Industria. En razón de lo anterior, este índice debe ser de particular interés para evaluar la implementación de dicha política.

[13] El ranking del GCI 2018 puede ser consultado en https://ncsi.ega.ee/ncsi-index/

[14] El CSIRT es el Equipo de Respuesta ante Incidentes de Seguridad Informática, del Gobierno de Chile. Pero la sigla es de uso común en la comunidad de seguridad informática y obedece al nombre en inglés para este equipo de respuesta, computer security incident response team.

[15] Los cinco pilares de la GCA son: técnico, legal, organizacional, cooperación y creación de capacidad.

TECNOLOGÍA 5G Y CIBERSEGURIDAD: ALGUNOS DESAFÍOS

Sin duda, la implementación de la tecnología 5G representa un gran desafío para cualquier Estado, puesto que para ello concurren aspectos legales, técnicos, comerciales y otras dimensiones o varibles que podrían condicionar su adopción. En ese sentido, el caso nacional presenta algunas ventajas. En el año 2022, justo cuando se inicie la implementación de la tecnología 5G en Chile, al Estado le corresponderá difundir una actualización de la Política Nacional de Ciberseguridad. En consecuencia, se encontrará en un importante punto de inflexión, que representaría una oportunidad para seguir avanzando sustancialmente en materias de ciberseguridad.

La actual Política Nacional de Ciberseguridad se estructuró considerando 5 objetivos de largo plazo (con horizonte al año 2022) y 41 medidas de política públicas que fueron pensadas para ser ejecutadas en el período 2017-2018, las que contribuyen al logro de los objetivos de largo plazo (MININT, 2017), medidas que se han ido cumpliendo de manera gradual.

De lo anterior se desprende que uno de los mayores desafíos que enfrentan los países, es la formulación de políticas públicas y normas legales que permitan consolidar una institucionalidad en materia de ciberseguridad. Las políticas públicas sobre la materia tienden a orientar la adopción de esta nueva tecnología en sincronía con otras iniciativas públicas (tecnología 5G y transformación digital del Estado, por ejemplo), mientras que una ley marco de ciberseguridad básicamente permite garantizar que la implementación del 5G se realice de acuerdo a los estándares y objetivos que se determinen, que se estructuren sistemas de incidentes informáticos de nivel nacional y se establezcan las responsabilidades en la materia.

El espectro legal vinculado a la tecnología 5G es bastante amplio. En efecto, el desafío para los estados está en articular todos aquellos aspectos que se relacionen con la ciberseguridad y las ventanas de oportunidad que generará el 5G. Así, la legislación sobre delitos informáticos, sobre protección de datos

personales y sobre infraestructura crítica de ciberseguridad, pasan a tener prioridad en las agendas de ciberseguridad.

La rápida evolución tecnológica de las materias que se abordan, su complejidad y especificidad inherente y los riesgos y amenazas a la seguridad nacional que se visualizan, hacen imperativo que la ciberseguridad sea abordada como política integral de largo plazo, una verdadera política de Estado.

Al respecto, conviene revisar lo que propone Elsa Kania en un estudio realizado como parte del proyecto *Securing Our 5G Future*, del Centro para una Nueva Seguridad en América (CNAS) que aborda los desafíos del 5G en un mundo globalizado y competitivo. En su trabajo, la investigadora entrega cinco recomendaciones para el mejoramiento de las políticas relacionadas con el 5G en Estados Unidos, a propósito de las tensiones entre dicho país y China por la materia (Ver Cuadro 2).

Si bien las recomendaciones son específicas para la realidad de Estados Unidos, conviene revisar algunas de ellas y extrapolarlas al caso nacional. Por ejemplo, en el segundo punto se señala que se debe prever que las futuras redes 5G sean seguras por diseño desde el principio. Dado que el año 2022 supone un punto de partida marcado por la implementación de la tecnología 5G y una nueva Política Nacional de Ciberseguridad, la fecha se presentaría como un plazo prudente para asegurar un diseño inicial que permita explotar las potencialidades de las redes 5G, pero protegiendo a sus usuarios y al propio Estado.

En ese sentido, sería factible incluso, ralentizar el avance en la materia si la seguridad así lo demanda.

Cuadro 2

Recomendaciones y consideraciones para políticas públicas

1) Priorizar e invertir en 5G como base para la competitividad.
2) Prever que las futuras redes 5G sean seguramente diseñadas desde el principio.
3) Concurso de liderazgo e innovación tecnológica dentro y más allá de 5G.
4) Buscar una coordinación más estrecha y una innovación colaborativa con aliados y socios.
5) Prepararse para aprovechar las externalidades positivas y mitigar las externalidades negativas del 5G.

Nota. Elaboración propia a partir de la traducción del texto de Elsa B. Kania (2019), *Securing Our 5G Future: The Competitive Challenge and Considerations for U.S. Policy,* pp. 15-22.

Por otra parte, Kania revisa los riesgos y preocupaciones de seguridad asociadas al 5G. Al respecto, se muestra escéptica de los intereses de las empresas chinas proveedoras de los servicios 5G y concluye que "aquellos países que eligen opciones menos seguras o dan prioridad a la facilidad y rapidez de implementación pueden encontrar mayores riesgos y mayores costos en el futuro"[16] (Kania, 2019, p. 13). De su escepticismo y preocupaciones, se desprende que los nuevos riesgos y amenazas que surgen a partir de la tecnología 5G no pueden seguir siendo abordados por los países solo como un avance tecnológico más, y actualizando someramente sus políticas.

Así, las evidentes implicaciones que genera la nueva tecnología 5G para los estados, guardan relación con nuevos riesgos y amenazas a la seguridad de estos.

En línea con lo anterior, otra implicancia relevante de la tecnología 5G, corresponde al desarrollo de capacidades estratégicas de Ciberdefensa y las políticas públicas asociadas. En tal sentido, Chile ha dado un paso importante puesto que la Política Nacional de Ciberdefensa incluye la disposición de creación de un Comando Conjunto de Ciberdefensa dependiente del Jefe del

[16] Traducción del autor.

Estado Mayor Conjunto, con la responsabilidad de la planificación y ejecución de operaciones militares conjuntas de ciberdefensa.

Más aún, la tecnología 5G podría incluso sugerir que los estados formalicen estrategias nacionales de ciberseguridad y/o de ciberdefensa, que permitan articular todos los medios y establecer la manera de lograr los objetivos que la política establezca. La transversalidad de la materia, los múltiples actores que intervienen en la estructura de ciberseguridad del país y la inmediatez de las acciones en el plano informático, harán que los estados pierdan la iniciativa en el ambiente de la información si no logran articular todas sus capacidades frente a los nuevos riesgos y amenazas que se visualizan en el horizonte, algunas incluso insospechadas.

Si bien un conflicto armado interestatal tradicional, al más puro estilo clausewitziano, no se puede descartar, las probabilidades de ocurrencia son menores en comparación con fenómenos como la subversión, el terrorismo, los conflictos de baja intensidad, la insurgencia, la narcoactividad, las guerrillas, el crimen organizado transnacional, entre otros.

En ese plano, pareciera que el paradigma de las guerras industriales entre estados ha cambiado definitivamente. Diversas teorías dan cuenta de ello. De acuerdo a lo que propone Rupert Smith en su obra *The Utility of the Force*, el nuevo paradigma de la guerra entre la gente es el sello de los conflictos modernos (Smith, 2005). Martin Van Creveld coincide con la evolución que plantea Smith y señala, en *La Transformación de la Guerra*, que “los intentos de los estados por mantener el monopolio de la violencia están tambaleándose” (Van Creveld, 2007, p. 261).

La violencia, por tanto, se estaría dirigiendo hacia los civiles y no precisamente hacia aquellos que por años ostentaron el uso legítimo de las armas. Y es aquí donde el ciberespacio cobra relevancia como medio para desarrollar la *guerra de la información*, un fenómeno donde la figura del combatiente tradicional se desdibuja, las fronteras desaparecen y los tiempos se acortan hasta casi la

inmediatez. Las acciones, muchas veces sin elevados recursos, son inmediatas y con efectos catastróficos, incluso con la capacidad de generar daño físico. Así, se estima que el logro de la iniciativa en el ambiente de la información se facilitaría para aquellos estados que hayan apostado por la formulación de una estrategia sobre la materia.

Pero para poder actuar en un ambiente complejo como el que se describe, se evidencian también desafíos para la educación. A partir de las ventajas de la tecnología 5G expuestas, es posible inferir que la población estará expuesta a una enorme cantidad de información y la interacción con aparatos que soporten estas capacidades puede que no siempre sea amigable. En ese contexto, será difícil para las personas poder gestionar la información que les sea útil para su trabajo o para su vida cotidiana. La búsqueda y discriminación entre información real o falsa, o útil e inútil, es algo que se debe educar y que es necesario para la solución de problemas. El campo de batalla futuro representa desafíos similares para los soldados y la gestión de su conocimiento, por lo que la solución de problemas de dicha índole debe adaptarse a las tecnologías disruptivas. Reino Unido, por ejemplo, ha considerado ello y específicamente, en el ámbito de la educación militar, publicó un texto doctrinario conjunto titulado *Understanding and Decision-making* (2016). El documento entrega orientaciones para el logro de un profundo entendimiento individual y luego un entendimiento compartido del ambiente operacional, como paso previo necesario para la toma de decisiones y la solución de problemas. La educación de las personas en general y en las diferentes áreas, en un mundo hiperconectado forma parte del desafío.

De igual manera, uno de los impactos de la tecnología 5G que tendrá efectos sobre la estructura nacional de ciberseguridad, será el aumento de la demanda de profesionales capacitados en el área de la ciberseguridad, lo cual paralelamente es una oportunidad para la fuerza laboral más joven. Un estudio titulado *(ISC)² Cybersecurity Workforce Study (2019)*[17]*,* planteaba que la brecha

[17] El estudio Cybersecurity Workforce Study 2019 de la (ISC)², y otras versiones, pueden ser consultados en https://www.isc2.org/Resource-Center?filter=featured

de profesionales en Latinoamérica es del orden de 600.000 personas, lo que equivale al 15% de la demanda (ISC^2, 2019). En la versión más reciente del mismo estudio se señala que, si bien la demanda ha disminuido producto de los efectos de la pandemia del COVID-19 sobre la economía, la brecha ha aumentado a un 17% para Latinoamérica (ISC^2, 2020). Como se aprecia, la brecha se ha incrementado, manteniéndose la tendencia de los últimos años.

Las especializaciones que más se requieren en el campo de la ciberseguridad, según Excequiel Matamala, Director del Centro de Ciberseguridad de la Asociación Chilena de Empresas de Tecnologías de Información (ACTI), "son seguridad de la información, protección de datos, auditoría de sistemas, gestión de riesgo tecnológico y continuidad operacional, entre otras" (Emol, 2020, p. 1). Por tanto, no es difícil proyectar que habrá problemas para la conformación de equipos de respuesta oportuna si, además, consideramos que los ataques son cada vez más rápidos y la capacidad de respuesta más lenta.

En definitiva, lo que se evidencia un verdadero cambio de paradigma para enfrentar la revolución de la tecnología 5G, debiendo "asumir la brecha actual" y orientar los esfuerzos hacia la ciber-resiliencia.

REFLEXIONES FINALES

En este trabajo se ha reflexionado en torno a las implicancias que podría tener el 5G para la seguridad. Al respecto, se han revisado aspectos de políticas públicas y los desafíos que supone la adopción de la tecnología 5G para los estados y para Chile en particular.

Con la llegada de la tecnología 5G, el mundo espera una verdadera revolución que cambiará la vida y el trabajo de las personas. En ese contexto, propio de la 4RI y particularmente de la revolución digital, no cabe duda que la tecnología 5G permitirá dar un gran paso en materia de conectividad, favoreciendo el desarrollo del Estado y su población.

No obstante, como se ha expuesto, desarrollo no es sinónimo necesariamente de seguridad. En ese sentido, se ha hecho énfasis en exponer los riesgos y

amenazas a los que se estarán expuestos los estados y específicamente lo que ello representa para la seguridad nacional.

A partir de lo anterior, podemos indicar que se ha respondido a la interrogante que orientó el trabajo, estableciéndose que existen implicancias relacionadas con materias jurídicas, educativas y no solo las que atañen directamente a la ciberseguridad, sino que también otras que se relacionan indirectamente con la transformación digital; también, con la necesaria actualización y monitoreo de un panorama de riesgos y amenazas, que se hace difícil de mensurar por la rapidez de los cambios; así como la necesidad de personal capacitado en el área de la cibernética, que tendrá efectos sobre la estructura de ciberseguridad pública y privada del país.

La discusión aquí planteada permite reflexionar respecto de uno de los avances más significativos en materia de TICs que se espera para los próximos años en el marco de la 4RI, que facilita la toma de consciencia por parte de la comunidad académica respecto a esta temática, transitando a un entorno cada vez más ciber-resiliente.

REFERENCIAS

Ball, D. (2011). China's Cyber Warfare Capabilities. *Security Challenges, 7*(2), 81-103. https://www.jstor.org/stable/26461991?seq=1#metadata_info_tab_contents

Baños, P. (2017). *Así se domina el mundo*: desvelando las claves del poder mundial. Madrid, Editorial Ariel.

BBC (2020). *Por qué algunos países prohíben la tecnología del gigante chino.* BBC News. https://www.bbc.com/mundo/noticias-53413017

Carrillo, J., Marco de Lucas, J., Dueñas, J., Cases, F., Cristino, J., González, G. y Pereda, L. (2013). Big Data en los entornos de Defensa y Seguridad. *Documento de investigación 03/2013*. Instituto Español de Estudios

Estratégicos [IEEE]. http://www.ieee.es/Galerias/fichero/docs_investig/DIEEEINV03-2013_Big_Data_Entornos_DefensaSeguridad_CarrilloRuiz.pdf

Centro de Estudios Estratégicos. (2018). *La Ciberguerra, sus impactos y desafíos*. Academia de Guerra del Ejército de Chile.

Corral, D. (2020). 5G, una carrera por la hegemonía y el futuro con muchos beneficios´. *Documento Marco 07/2020*. Instituto Español de Estudios Estratégicos [IEEE]. http://www.ieee.es/Galerias/fichero/docs_marco/2020/DIEEEM07_2020DAVCOR_5G.pdf

Defense Science Board. (2019). *Defense Applications of Fifth Generation Network Technology*. Department of Defense [DoD]. https://www.hsdl.org/?abstract&did=828623

Emol.com. (2017). *¿Estás listo para un cyberataque? Chilenos estamos entre los menos preparados de Latinoamérica.* Portal PYME. Entrevista a Eduardo Parada, Gerente de Ingeniería de la Consultora TI Vector para *Emol.com.* https://pyme.emol.com/9886/estas-listo-cyberataque-chilenos-estamos-los-menos preparados-latinoamerica/

Emol.com. (2020). En Chile hay escasez de capital humano en ciberseguridad. *Ediciones Especiales. Emol.com.* https://seguridaddigital.emol.com/noticias/en-chile-hay-escasez-de-capital-humano-en-ciberseguridad/

European Union Agency for Cibersecurity, (2019), *ENISA Threat Landscape For 5G Networks.* https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks

Fortinet. (2020). *Threat Intelligence Insider Latin América, Reporte para Chile, tercer trimestre de 2020.* https://www.fortinetthreatinsiderlat.com/es/Q3-2020/CL/html/trends

Gallardo, M. (2019). Riesgos y amenazas para la seguridad multidimensional. *Transformaciones Estratégicas Globales, Retos y Repercusiones*. Centro de Estudios Estratégicos de la Academia de Guerra, pp. 65-83

Huawei. (2019). *5G Antenna White Paper: New 5G, New Antenna*. Shenzhen, Huawei Technologies Co. Ltd.

ITU. (2018). *Global Cybersecurity Index (GCI) 2018.* Ginebra, Suiza: ITU Publications. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

ISC2. (2019). *(ISC) 2 Cybersecurity Workforce Study, 2019.* https://www.isc2.org/Resource-Center?filter=featured

ISC2. (2020). *(ISC) 2 Cybersecurity Workforce Study, 2020.* https://www.isc2.org/Resource-Center?filter=featured

Kania, E. (2019). *Securing Our 5G Future: The Competitive Challenge and Considerations for U.S. Policy*. Center for a New American Security. https://www.cnas.org/publications/reports/securing-our-5g-future

La Nación. (2020). *Ciberataque a Banco Estado habría sido provocado por hackers de Corea del Norte*. http://www.lanacion.cl/ciberataque-a-bancoestado-habria-sido provocado-por-hackers-de-corea-del-norte/

Leiva, R. (2017). Ciberdefensa ¿Hacia un nuevo eje estratégico? *Revista Ensayos Militares, 3* (1), 77-92.

McGuinness, D. (2017). *Cómo uno de los primeros ciberataques de origen ruso de la historia transformó a un país*. BBC Mundo. https://www.bbc.com/mundo/noticias-39800133

Mena, J. (2020). *Ventajas, desventajas y mitos de la tecnología 5G*. Universidad Autónoma de Occidente. https://www.uao.edu.co/ingenieria/ventajas-desventajas-y-mitos-de-la-tecnologia-5g/

Ministerio de Defensa de Chile. (2018). *Política Nacional de Ciberdefensa*. Ministerio de Defensa [MINDEF]. https://www.diariooficial.interior.gob.cl/publicaciones/2018/03/09/42003/01/1363153.pdf

Ministerio del Interior. (2017). *Política Nacional de Ciberseguridad*. Ministerio de Interior [MININT]. https://www.ciberseguridad.gob.cl/media/2017/05/PNCS CHILE-FEA.pdf

Ministerio del Interior. (2019). *Fue Publicado el Índice de Ciberseguridad Global (GCI) para 2017-2018*. Ministerio de Interior [MININT]. https://www.ciberseguridad.gob.cl/noticias/fue-publicado-el-indice-de-ciberseguridad global-gci-para-2017-2018/

Ministry of Defense. (2016). Joint Doctrine Publication 04: Understanding and Decision-making. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/584177/doctrine_uk_understanding_jdp_04.pdf

MITRE. (2017). *Cyber Resiliency FAQ*. McLean. The MITRE Corporation. https://www.mitre.org/sites/default/files/PR_17-1434.pdf

NCSI. (2020). *Ranking National Cyber Security Index.* https://ncsi.ega.ee/ncsi index/

Purdy, A., Yordanov, V. y Kler, Y. (2020). Dont't Trust Anyone: The ABCs of Building Resilient Telecommunications Networks. *PRISM, 9* (1), 115-129.

RoiPress. (2020). *Impacto de COVID-19 en el cibercrimen en Chile*. https://roipresscanalnoticias.blogspot.com/2020/09/chile-sufrio-mas-de-525-millones-de.html

Samsung. (2020). *6G. The Next Hyper-Connected Experience for All*. Samsung Research. https://cdn.codeground.org/nsr/downloads/researchareas/6G%20Vision.pdf

Smith, R. (2005). *The Utility of Force, the art of war in the modern world*. Allen Lane.

Schwab, K. (2016). *La Cuarta Revolución Industrial*. Editorial Debate.

Unión Europea. (2019). *ENISA Threat Landscape For 5G Networks.* ENISA. https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks

U.S. Cyber Command. (2020). *U.S. Cyber Command History*. https://www.cybercom.mil/About/History/

Van Creveld, M. (2007). *La Transformación de la Guerra, la más radical reinterpretación del conflicto armado desde Clausewitz*. José Luis Uceda.

Vego, M. (2009). *Joint Operational Warfare: Theory and Practice*. U.S. Naval War College.

World Economic Forum [WEF]. (2021). *The Global Risks Report 2021.*

https://www.weforum.org/reports

DISUASIÓN Y USO DE LA LEGÍTIMA DEFENSA EN EL CIBERESPACIO

Deterrence and use of self-defense in the cyberspace

MAY. Rodrigo Kinast Werner *

Resumen: El presente artículo pretende establecer algunos argumentos con respecto a la aplicabilidad de la política disuasiva en relación a las nuevas amenazas que se presentan en el ciberespacio. Además de lo anterior, tiene la intención de evidenciar la articulación del arte de la estrategia de la disuasión al emplearse en conjunto con la ciencia y la tecnología. Junto con ello, se discuten las complejidades para justificar el empleo de la legítima defensa frente a una agresión en el ambiente digital, considerando las características del ambiente de la información y de este dominio.

Palabras claves: disuasión, ciberdefensa, ciberataque, legítima defensa, Estado

Abstract: This article aims to establish some arguments regarding the applicability of deterrence policy in relation to new threats in cyberspace. Likewise, how it is articulated the art of deterrence strategy with science and technology is analyzed. In addition, complexities to establish the use of self-defense against a ciberattack or aggression in the digital environment are discussed, considering the characteristics of this domain.

Key words: deterrence, cyber defense, cyberattack, self-defense, State

* Oficial del Arma de Infantería. Oficial de Estado Mayor. Magíster en Ciencias Militares con mención en Gestión Estratégica. Magíster en Inteligencia Económica. Profesor Militar de Academia de la asignatura de Táctica y Operaciones. Actualmente se desempeña como Comandante de Unidad de Combate de la Fuerza Terrestre del Ejército. ✉rkinastw@gmail.com

INTRODUCCIÓN

El siglo XXI se ha caracterizado por un aumento exponencial de las Tecnologías de la Información y las Comunicaciones (TIC), lo que ha permitido la optimización y automatización de los procesos, generando además, la interrelación entre los sistemas informáticos y las bases de datos, para el empleo de la información. Ello ha producido la masificación y ubicuidad en el uso de internet, originando un nuevo escenario o dimensión denominado “ciberespacio”, definido en la Política Nacional de Ciberseguridad (2017) y en la Doctrina Nacional Conjunta 2-11 (2017) como “el ambiente intangible compuesto por las infraestructuras tecnológicas, los componentes lógicos de la información y las interacciones sociales que se verifican en su interior", la que se suma a los tradicionales dominios de tierra, aire, mar y espacio.

En relación con lo anterior, los desafíos en el uso y explotación del ciberespacio son cada vez mayores. Es complejo detectar los orígenes, causales y motivaciones de un ciberataque, los cuales pueden proceder de diversas organizaciones criminales, individuos aislados o incluso desde otros estados. Dichos ataques, pueden generar grave impacto en el funcionamiento de las instituciones, organismos y sistemas, tanto públicos como privados, afectando directamente o indirectamente al Estado y en consecuencia a la población.

Tal como lo plantea la Doctrina Nacional Conjunta 2-11 (2017), la diversidad de amenazas que pueden afectar el estado de normalidad en el uso del ciberespacio, obligan a que distintos actores, tanto públicos como privados, desarrollen una perspectiva holística e integradora que permita disminuir las vulnerabilidades y enfrentar estos riesgos y amenazas; siendo el Estado, el encargado de cumplir el rol fundamental de dirigir los esfuerzos, mediante políticas y directrices claras que permitan el empleo eficaz de las capacidades, con la finalidad de proteger los atributos de la información, su confidencialidad, integridad y disponibilidad.

Al mismo tiempo, es pertinente tener presente que para avanzar en esta materia, se requiere crear soluciones que trasciendan lo puramente tecnológico. Para esto

es necesario un marco legal, colaboración pública y privada y participación y educación de la población. Lo anterior, complementado además, con nuevas herramientas tecnológicas capaces de neutralizar o mitigar ataques cibernéticos cada vez más sofisticados.

En este contexto, el Estado de Chile ha arbitrado desde hace algunos años medidas concretas, destinadas a redituar los beneficios de las nuevas tecnologías. Una de ellas fue la denominada Agenda Digital (AD2020), lanzada el año 2015 y que contenía cinco ejes principales en política pública, con diferentes ejes de acción: derechos para el desarrollo digital, conectividad digital, gobierno digital, economía digital y competencias digitales (AD2020, 2015). Específicamente el eje de gobierno digital, ordenó la creación de una estrategia de ciberseguridad, la que fue presentada en el año 2017 y se encuentra vigente hasta la fecha. Esta definió distintas medidas, siendo una de ellas, la elaboración de una Política de Ciberdefensa (Política Nacional de Ciber Seguridad, 2017), la cual fue promulgada a fines del año 2017, con los siguientes principios básicos:

> El respeto del derecho internacional público, incluyendo la abstención del uso y la amenaza del uso de la fuerza, la legítima defensa y el respeto a la soberanía, la promoción de la democracia y el respeto por los derechos humanos y la protección de la población, de los intereses nacionales y de la integridad nacional. (Política de Ciberdefensa, 2018, p. 3)

En relación con los principios descritos, se evidencia que la Política de Ciberdefensa posee total coherencia y compatibilidad con los siete principios de la Política de Defensa Nacional declarados en el Libro de la Defensa 2017, en especial en cuanto a la aplicación del derecho a la legítima defensa y respecto al uso de sus capacidades (Ministerio de Defensa, 2017, p. 96). En este contexto y considerando esta vinculación, surge la interrogante ¿Son aplicables la disuasión y la legítima defensa como modalidades de empleo de los medios de la Defensa en el dominio del ciberespacio?

Con la intención de dar respuesta a ello, el presente artículo aborda dos de las

tres modalidades de empleo de la Defensa (disuasión, legítima defensa y cooperación internacional). Inicialmente se enfoca en describir la teoría de la disuasión y su aplicabilidad en el dominio del ciberespacio y, posteriormente, evidenciar bajo el amparo de la legítima defensa la factibilidad de empleo de ciber capacidades.

TEORÍA DE LA DISUASIÓN

La teoría de disuasión en el marco estratégico contemporáneo empezó a adquirir importancia a principio de los años 50', dado el crecimiento del armamento nuclear (Chinchilla, 2018). Pero más que una teoría, se trata de un supuesto sobre la conducta de un agresor, cuya utilización abarca diversos campos, como la economía, el derecho, la sociología, la psicología social y la criminología (Bravo, 2017). El supuesto básico de la teoría puede ser planteado de la siguiente forma: a nivel individual, la conducta ilegal puede ser controlada por la amenaza de recibir sanciones ciertas, severas y rápidas. La evidencia acerca de estos tres factores (certeza, severidad y rapidez) no es concluyente, pero es probable que solo el primero de los tres (certeza de castigo/pena) sea un disuasor fuerte, la percepción de la severidad del castigo o pena es un disuasor suave, y la celeridad de castigo o pena parece no ser un disuasor.

En general, ya sea de individuos o de autoridades tomando decisiones en nombre de un Estado, se acepta que la disuasión, de existir, debe hacerlo en la mente del agresor o de la víctima que considera devolver el ataque. La evidencia en el párrafo anterior es, por tanto, aplicable tanto en el caso de estados como de personas; sin embargo, existen consideraciones adicionales que es necesario realizar en el caso de la disuasión como estrategia entre estados.

ESTRATEGIA DE DISUASIÓN EN CONFLICTOS EN EL AMBIENTE FÍSICO

Una estrategia de disuasión es una política declarada de un Estado. Paul Nitze distingue entre la política declarada y la política de acción. Mientras la primera se refiere a "declaraciones públicas de objetivos", la segunda se refiere a "objetivos y planes militares concretos para emplear la fuerza existente" (Nitze citado en Arenas, 2013, p.

223). Según el Libro de la Defensa Nacional de Chile (2017), la disuasión comprende tanto un efecto como la acción que lo causa, por tanto:

> Es un efecto por cuanto corresponde a una dimensión psicológica o subjetiva que se produce en un potencial adversario. La disuasión no pretende paralizar toda acción contraria al interés nacional, sino generar en el potencial adversario la convicción que el costo de transferir coactivamente contra intereses vitales propios será más alto que los beneficios de obtener. (Libro de la Defensa Nacional de Chile, 2017, p. 132)

Esta es una de las variadas definiciones sobre disuasión que declaran los estados. Generalmente, estas se conforman de siete elementos comunes, a saber:

a. Un interés a proteger: todo Estado que emplea una estrategia disuasiva lo hace para proteger algún interés específico, como su población, su soberanía o su infraestructura crítica (servicios básicos, caminos, recursos económicos, entre otros).

b. Una declaración (“No hagas X, o de lo contrario te ocurrirá Y”): por supuesto, puede haber múltiples acciones X y múltiples medidas Y.

c. Reafirmación: en términos lógicos, esta es la declaración inversa de la anterior. Si A no realiza X, entonces de seguro no ocurrirá Y. En la práctica, esto tiene que ver con asegurar a A que B no incurrirá arbitrariamente en medidas de respuesta si no existe una amenaza real de parte de A.

d. Medidas de negación: es la parte defensiva de la disuasión. Consiste tanto en aquellas medidas tomadas para prevenir que X ocurra, así como las medidas tomadas para disminuir o anular los efectos de X si este llegara a tener éxito.

e. Medidas de castigo o respuesta: es la parte ofensiva de la disuasión. Consiste en las acciones que B ejecutará en respuesta a un ataque (es

f. decir, Y). El supuesto básico de una medida de respuesta es que el costo para el país agresor por la respuesta es mayor que el beneficio obtenido por el ataque, es decir, costo A (Y) > beneficio A(X).

g. Credibilidad: el país A debe creer que B es capaz de ejecutar la acción Y; de lo contrario, incurrirá de todas formas en el ataque.

h. Miedo: con esto se alude al temor que produce un ataque sobre la población afectada, es decir, al temor que puede producir Y sobre la población de A. (Bravo, 2017)

Estos siete factores conforman el medio en que opera la disuasión, pero hay que agregar el cálculo costo-beneficio que pondera todos los factores anteriores.

ESTRATEGIA DE DISUASIÓN DIGITAL

¿Cómo deben ser interpretados los conceptos anteriores, si se piensa en una estrategia de disuasión para el ciberespacio? A continuación, se interpretarán algunos de los elementos presentados previamente, con el fin de vincularlos con esta nueva dimensión.

Intereses a proteger

En el mundo digital también existen intereses que son necesarios proteger. Por ejemplo, actualmente existe preocupación entre los países de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) y la Organización de Estados Americanos (OEA), con respecto a la protección de la infraestructura crítica de información (ICI), la que es entendida en Chile como:

> Las instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya afectación, degradación, denegación, interrupción o destrucción pueden tener una repercusión importante en la seguridad, la salud, el bienestar de los ciudadanos y el efectivo funcionamiento del Estado y del sector privado. (Política de Ciberdefensa, 2018, p. 4)

Medidas de negación

De los tres componentes que componen el ciberespacio[1], un ataque digital explota dos de ellos; primero, las vulnerabilidades en los sistemas lógicos (software) y el segundo, por las limitaciones y sesgos en las personas (interacciones). Por lo tanto, la mejor forma de defender a un Estado y, por ende, a sus instituciones, es por medio de:

a. Búsqueda y reparación continúa de vulnerabilidades en los sistemas informáticos que forman parte de los intereses a proteger.
b. Capacitación y entrenamiento constante de las personas dentro del Estado y sus instituciones, para evitar que estas sean engañadas y divulguen información relacionada con el acceso a los sistemas.

Medidas de reprimenda

Una medida de respuesta digital necesariamente implica el empleo de una "ciberarma" en contra del atacante. Conforme a lo anterior, las medidas de respuesta constituyen la parte ofensiva de la disuasión. Por lo tanto, una medida de respuesta es, necesariamente, de naturaleza ofensiva, no defensiva. Algunos ejemplos de medidas que un Estado podría tomar en respuesta a un ciberataque son:

a. Medidas de respuesta operacionales: inyectar "malware" en los sistemas informáticos del oponente; utilizar una "botnet", con el objeto de lanzar un ataque de denegación de servicio[2] (DDos) sobre los sistemas del oponente; hacer uso de una vulnerabilidad en un sistema Supervisory Control And Data Acquisition[3] (SCADA) para producir fallas en los sistemas eléctricos, distribución de agua, control de tráfico aéreo, entre otros.

---

1 Ciberespacio es un ambiente compuesto por las infraestructuras tecnológicas, los componentes lógicos de la información y las interacciones sociales que se verifican en su interior (BPCS, 2015, p. 13).

2 Es un ataque donde muchos servidores llenan de peticiones un servidor, con la finalidad de que deje de funcionar.

3 Es un tipo de Sistema de Control Industrial que monitorea y ejecuta procesos industriales. Se utiliza en todo, desde la gestión y operación de centrales eléctricas hasta la fabricación de envoltorios de dulces.

b. Medidas de respuesta conductuales: capturar las credenciales de acceso a las autoridades civiles o militares del oponente y destruir la información de sus cuentas públicas o privadas; lanzar un ataque masivo de “phishing” sobre la población de otro país, con la intención de capturar sus credenciales de acceso a la banca y transferir dinero de forma masiva a otras cuentas, entre otros.

LA DISUASIÓN ENTRE ESTADOS ¿ES POSIBLE EN EL CIBERESPACIO?

A partir del análisis anterior, es posible aplicar la disuasión digital con ciertas consideraciones:

a. No es cuantificable: La disuasión digital difiere de la cantidad de armamento y personal que posea un Estado, no es algo “cuantificable”.

b. Nivel de desarrollo tecnológico: La disuasión digital no tiene sentido cuando un Estado no posee un desarrollo tecnológico considerable. Por ejemplo, no causaría el mismo efecto la disuasión hacia un estado con un bajo desarrollo tecnológico, en comparación a realizarla hacia otro que posee mayor desarrollo y nivel de implementación de las TIC.

c. El problema de la seguridad: Las vulnerabilidades son parte de las mismas instituciones y organizaciones que componen una nación. Es decir, para disuadir a un adversario no basta tener altas capacidades para ejercer el poder nacional, sino que es necesario contar con una infraestructura robusta, redundante y resiliente, condición que puede ser promovida por los ámbitos público y privado. De esta forma, desincentiva a un posible atacante de generar una agresión. Por ejemplo, si se declara que la capacidad de la Defensa Nacional puede resguardar la soberanía, la defensa tiene los medios para actuar ante una posible agresión enemiga; pero, lo anterior no ocurre de igual forma en el medio digital. La responsabilidad de lo que se desea proteger recae también en privados, por lo tanto, la labor de asegurar este ámbito le compete a un actor que se encuentra fuera del alcance de la defensa, si no es incluido en las políticas.

d. Cooperación internacional: los estados deben participar activamente en ejercicios conjuntos, seminarios, entre otros. En esta área, para lograr disuadir a potenciales amenazas es conveniente continuar los ejercicios de ciberseguridad, ejecutados tanto en la Organización del Tratado Atlántico Norte (OTAN), como también en Unión Europea (EU), con la finalidad de demostrar que es un actor válido, lo que constituiría un indicador para disuadir a un posible atacante, sea este un agente estatal, como no estatal[4]. Ejemplo de esta intención fue la participación de representantes del Ejército, Armada, Fuerza Aérea, Estado Mayor Conjunto y del Ministerio de Defensa Nacional de Chile, en conjunto con especialistas del US Army Cyber Command en la ejecución del primer Ejercicio Conjunto en Ciberdefensa entre ambos países. La actividad, que se desarrolló en la ciudad de Santiago entre 19 y el 23 de agosto, formó parte del acuerdo de cooperación entre Chile y Estados Unidos (Subsecretaría de Defensa, 2019).

En caso de no considerar alguno de los puntos antes presentados, la disuasión en este dominio resultaría menos eficiente y, por ende, un ataque podría ocurrir sin ser detectado a tiempo; por lo tanto, si se evidencia que un ciberataque masivo está ocurriendo contra la soberanía, sus habitantes, su infraestructura, o aquello que dañe sus intereses ¿Cómo se podrían poner en ejecución las capacidades en ciberdefensa del poder nacional?

Legítima defensa

Enfocándose en conceptualizar la legítima defensa como un derecho inmanente de los estados, es de suma importancia conocer que las normas jurídicas pueden ser interpretadas desde variadas perspectivas, siendo una de ellas el punto de vista de los resultados a los que conducen. En este contexto, el artículo 51° señala que:

[4] Agente no estatal: persona física o entidad que no actúa bajo la autoridad legítima de un Estado en la ejecución de actividades comprendidas en el ámbito de la presente resolución (S/RES/1540, 2004, p. 1).

> "Ninguna disposición de esta Carta menoscabará el derecho inmanente de legítima defensa, individual o colectiva, en caso de ataque armado contra un Miembro de las Naciones Unidas, hasta que el Consejo de Seguridad tome las medidas necesarias para mantener la paz y la seguridad internacionales". (ONU, 1945)

Lo anterior, puede ser interpretado desde dos perspectivas: una restrictiva y otra extensiva. La diferencia entre ambas radica en que la primera busca siempre la interpretación restrictiva; en otras palabras, la abstención al máximo del uso de la fuerza, estableciendo una clara diferencia con la interpretación extensiva, situación en la que el artículo 51° se puede emplear y justificar en más casos de los que ordena la norma; por ejemplo, bajo esta interpretación, además de reconocer la legítima defensa, se podría justificar también medidas de autoprotección e incluso los ataques preventivos.

Haciendo esta salvedad, se interpretará el derecho a legítima defensa de forma restrictiva a lo largo de este artículo.

Agresión

Sin embargo ¿Cómo se podría invocar el derecho a la legítima defensa? Antes de saber el cómo, es necesario conocer qué tipo de agresiones podrían conllevar el uso del derecho inmanente antes mencionado. En este sentido, la Asamblea General de la ONU, mediante la resolución 3314 de 1974, logró un acuerdo sobre una definición de acto de agresión. A continuación, se presenta un extracto de esta:

> "Con sujeción a las disposiciones del artículo 2° y de conformidad con ellas, cualquiera de los actos siguientes, independientemente de que haya o no declaración de guerra, se caracterizará como acto de agresión:

1. La invasión o el ataque por las fuerzas armadas de un Estado del territorio de otro Estado, o toda ocupación militar, aún temporal, que resulte de dicha invasión o ataque; o toda anexión, mediante el uso de la fuerza, del territorio de otro Estado o de parte de él.

2. El bombardeo por las fuerzas armadas de un Estado al territorio de otro Estado, o el empleo de armas por un Estado contra el territorio de otro Estado.

3. El bombardeo de los puertos o de las costas de un Estado por las fuerzas armadas de otro Estado.

4. El ataque por las fuerzas armadas de un Estado contra las fuerzas armadas terrestres, navales o aéreas de otro Estado, o contra su flota mercante o aérea.

5. La utilización de fuerzas armadas de un Estado que se encuentran en el territorio de otro Estado con el acuerdo del Estado receptor, en violación de las condiciones establecidas en el acuerdo o toda prolongación de su presencia en dicho territorio después de terminado el acuerdo.

6. La acción de un Estado que permite que su territorio, que ha puesto a disposición de otro Estado, sea utilizado por ese otro Estado para perpetrar un acto de agresión contra un tercer Estado.

7. El envío por un Estado, o en su nombre, de bandas armadas, grupos irregulares o mercenarios contra otro Estado de tal gravedad que sean equiparables a los actos antes enumerados, o su sustancial participación en dichos actos" (ONU, 1974).

En la resolución expuesta, se pueden apreciar los siete puntos en los que se considera, a modo de definición, qué se entiende por un acto de agresión entre estados o en su nombre, independiente de si existe una declaración de guerra o no. También se debe agregar que en el párrafo 4° de esta resolución, se aclara que la lista presentada engloba parte importante de los aspectos definitorios, pero pudiesen ser otros más no incluidos y, por lo tanto, el Consejo de Seguridad puede determinar otros actos, de conformidad con la Carta, que constituyen agresión.

Actores y legítima defensa

Entonces ¿Cómo se podría interpretar el concepto recién expuesto ante un ciberataque masivo a la soberanía de un Estado y, por ende, que implique el

despliegue de sus capacidades en ciberdefensa? Antes de contestar esta pregunta, es necesario plantear el problema de determinar qué actores podrían realizar este ataque.

Teniendo en cuenta los diferentes actores (tanto estatales como no estatales), es posible analizar la aplicabilidad del concepto de agresión por medio del uso de ciberarmas. Además, se debe agregar otro aspecto fundamental en el ciberespacio, este es que existe un problema para determinar de dónde proviene un ataque (locación), como también quién lo realizó (actor). Por lo tanto, se genera el desafío de determinar la atribución (identificar al actor) y la motivación (intereses y vinculaciones), elementos esenciales para aplicar el derecho internacional público con la finalidad de sancionar este tipo de ataques.

CASOS DE ESTUDIO ¿SE HA UTILIZADO LA INVOCACIÓN DEL DERECHO A LA LEGÍTIMA DEFENSA EN EL CIBERESPACIO?

A continuación, se presentan tres casos de ciberataques masivos contra estados, y se verifica la posible invocación del derecho a la legítima defensa.

Estonia

El primer ataque informático masivo ocurrido contra un Estado le aconteció a Estonia, el 27 de abril del 2007, prolongándose por 22 días, ocasionando la paralización de los servicios financieros, el comercio y las comunicaciones nacionales, entre otros.

En este contexto, para entender cómo se gestó y desarrolló esta crisis, es necesario tener en consideración que Estonia era un pequeño Estado que pertenecía a la Ex Unión Soviética y que en 1991 comenzó a ser un país independiente. Con tan solo 1.3 millones de habitantes, esta nación ha hecho de su infraestructura digital un motivo de orgullo nacional, ya que antes del ataque, algunas de sus iniciativas de desarrollo digital eran:

En el año 2000, el gobierno declaró Internet como un Derecho Humano Básico, como también suprimió el uso de papel en todas las dependencias estatales,

remplazándose por un soporte electrónico, e incluso los gastos efectuados en el presupuesto general del Estado se pueden seguir en Internet en tiempo real. El 90% de los ciudadanos estonios posee una ID Card, que le permite acceder a diferentes servicios, como por ejemplo, transporte público, salud, validar elecciones electrónicas, entre otros.

Fue el primer país que inició pruebas de voto electrónico a través de Internet en 2004, lo que permitió que las elecciones de 2007 se realizarán vía web a través de ordenadores.

El 98% de las transacciones bancarias del país son digitales. Del mismo modo, el 99% de los casi 1800 trámites oficiales estatales se pueden realizar de manera online.

Estas son tan solo algunas medidas que llevaron a Estonia, en menos de un cuarto de siglo, a ser el país con mayor desarrollo digital en el mundo, pero también el más propenso a las nuevas amenazas en el ciberespacio.

En abril de 2007, el gobierno estonio movió un memorial de la guerra rusa, “el soldado de bronce de Tallin”, desde una intersección céntrica de la capital Tallin hacia un cementerio militar. Los ciudadanos veían la estatua que se emplazaba en ese lugar desde 1947 como un recuerdo de la opresión rusa, pero los ciudadanos de ascendencia y etnia rusa vieron la relocalización de la estatua como una afrenta. Parte de la población étnicamente rusa protestó en las calles: las revueltas duraron dos días, hasta que fueron diluidas por la policía local. Si bien los disturbios fueron controlados, ese mismo día comenzaron una serie de ataques DDoS en contra de la infraestructura gubernamental, financiera y de los medios de comunicación, ya que muchos de los servidores que usualmente antes del ataque recibían 1000 visitas diarias, durante el ataque pasaron a recibir 2000 solicitudes por segundo.

El Gobierno estonio rápidamente se percató que estaba bajo ataque, y conformó un Computer Emergency Response Team (CERT), pero los ataques con el pasar del tiempo cambiaron de forma y se volvieron más sofisticados. Como respuesta,

Estonia cerró sus fronteras en Internet, de manera que los usuarios dentro del país pudieran seguir utilizando los servicios internos. Incluso se solicitó apoyo a Organización del Tratado del Atlántico Norte (OTAN), ya que Estonia es miembro de esta alianza político-militar, y en consecuencia podía invocar la legítima defensa colectiva para atacar o disuadir al atacante de seguir con la agresión.

El gobierno estonio acusó a Rusia del ataque porque según el Ministerio de Defensa descubrió instrucciones circulando por web rusas de cómo unirse al ataque. Rusia negó la responsabilidad como nación sobre el incidente (McGuinness, D., 2017).

Guerra de Osetia del Sur (Georgia)

Luego de la disolución de la URSS, tres regiones que pertenecían a la República Socialista de Georgia reclamaron su independencia, esto generó una serie de conflictos en la región de Osetia del Sur, Abjasia y Adzaria, donde finalmente las fuerzas rusas intervinieron como fuerzas de paz para estabilizar esta zona de importancia estratégica.

En este contexto, el presidente Mijail Saakashvili, al llegar al poder fomentó el nacionalismo georgiano, cambiando su orientación política hacia occidente con una clara posición anti-rusa, lo que se vio reflejado en la solicitud del retiro de las fuerzas de paz rusas para ser reemplazadas por fuerzas de la OTAN; por su parte, Rusia aumentó su grado de influencia en la zona con un mayor acercamiento y protección hacia las regiones de Osetia, Abjasia y Adzaria.

El gobierno georgiano le ofreció autonomía a la región de Osetia del Sur, la que fue rechazada, ya que ellos buscaban su independencia total. Es importante señalar que la mayor parte de la población de esta región es de origen ruso, por lo que Georgia acusó a Rusia de promover el separatismo.

Los hechos anteriormente nombrados provocaron la desestabilización de la zona, con un incremento del asedio por parte de las fuerzas georgianas sobre las fuerzas rebeldes de Osetia, aumentando la militarización de la región, tanto por fuerzas georgianas como por fuerzas rusas.

El 8 de Agosto de 2008 las fuerzas armadas georgianas iniciaron un ataque sobre la localidad de Tsjinval, siendo este el inicio de la guerra en Osetia del Sur.

Es en este conflicto donde se implementó el uso del ciberespacio como una nueva dimensión, ejecutando ciberataques simultáneamente a los ataques militares convencionales. A pesar de que estos ataques no afectaron la infraestructura crítica, sí contribuyeron a las operaciones que buscaban el dominio de la información y propaganda (INFOOPS), principalmente con la denegación de servicios (DDoS) sobre las páginas oficiales del gobierno de Georgia, además de modificar algunos sitios web con ataques "defacement"[5] donde cambiaron la cara del presidente georgiano por la de Adolf Hitler.

Ante estos ataques, presumiblemente efectuados por piratas cibernéticos y hackers rusos (Markoff, 2008) Georgia solicitó cooperación internacional para solucionar esta crisis informática.

Irán (Stuxnet)

¿Es posible vulnerar los sistemas SCADA[6]? o ¿Es viable atacar a una red que "no" esté conectada a Internet? La respuesta a ambas interrogantes es "sí", y uno de los casos más estudiados ocurrió en el año 2010, cuando la planta nuclear de Natanz, en Irán, fue atacada por un "malware"[7].

El malware que atacó la planta fue bautizado como Stuxnet, y se infiltró en los sistemas hasta llegar a comprometer directamente los controladores lógicos programables PLC (Siemens), que manejaban los parámetros de las centrifugadoras de uranio, ya que Stuxnet -mediante una estructura altamente sofisticada- contenía cuatro "zero days"[8], como también certificados de autentificación válidos para Windows, entre otras particularidades, haciendo de

[5] Se conoce como ataques defacement a aquellos donde se toma el control de la página web y se modifica su apariencia.

[6] SCADA es el acrónimo del concepto en inglés "Supervisory Control And Data Acquisition", el que se utiliza para realizar softwares que permiten controlar y supervisar procesos industriales a distancia.

[7] Software malicioso que se crea para infiltrarse en programas y dispositivos con el fin de causar daño.

[8] Zero-day, es un tipo de ataque que explota una vulnerabilidad previamente desconocida.

este código malicioso un "gusano"[9] que se propaga a través de las redes sin la intervención del usuario. Igualmente, se replicaba a través de dispositivos USB[10] extraíbles, sin levantar ninguna sospecha, ni alarma.

¿Pero cómo se infiltró, si estas redes son cerradas? Al respecto, se manejan diversas hipótesis. Una de ellas, de acuerdo a la firma de seguridad cibernética Symantec (BBC, 2015) señala que Stuxnet llegó al programa nuclear iraní desde una memoria USB infectada a la red. Posterior a esto, el "gusano" escaló, realizó movimientos laterales y creó persistencia, llegando a las PLC ya mencionadas.

El uranio que se encuentra en los yacimientos mineros no vale por sí mismo para el uso nuclear, ya que lo que se extrae de la tierra es una mezcla sólida de dos tipos de uranio: 235 y el 238, pero sólo el primero sirve para fabricar combustibles, bombas, entre otras utilidades. Teniendo en cuenta que en el planeta se encuentra una concentración del 99,3% del uranio 238 y solamente un 0,7% del tipo 235, es necesario separarlos. La técnica más habitual es el centrifugado, donde primero se pasa todo el uranio a modo gaseoso (se convierte en hexafloruro de uranio mediante un proceso químico) el que luego se introduce en una centrifugadora. Ahí es donde el uranio 238, más pesado, comienza a girar en la periferia, al tiempo que el 235, más ligero, queda más al centro.

El malware atacó los parámetros de las PLCs, manipulando las velocidades y periodos de tiempo dispuestos, pero sin dar señales en los monitores administrados por los operarios de dichas centrifugadoras.

En consecuencia, estallaron 984 centrifugadoras, por lo tanto, este hecho comprueba la posibilidad que un ataque informático pueda destruir infraestructura física y en un futuro podría afectar directamente la integridad de las personas.

En los tres casos descritos, se estima que los estados afectados, dada la complejidad de efectuar la atribución (identificar los causantes de los ataques), ni

[9] Software malicioso el que una vez infiltrado en un dispositivo se propaga hacia otros.

[10] USB es el acrónimo del concepto Universal Serial Bus. Corresponde a un dispositivo de comunicación que conecta y provee alimentación eléctrica entre computadoras y otros dispositivos electrónicos.

su motivación (intereses y vinculaciones), reaccionaron por medio de la diplomacia y las comunicaciones estratégicas, viéndose imposibilitados de invocar el derecho a la legítima defensa. Estonia, acudió a solicitar la defensa colectiva, trayendo expertos de la OTAN, es decir a través de la cooperación internacional. Georgia, por su parte, solicitó ayuda internacional para solucionar la crisis informática que habían provocado los ataques. Por su parte, Irán denunció el hecho públicamente.

Finalmente, se evidencia un problema que se deriva de la atribución. Hay grupos sin motivación, ni vinculación estatal que pueden realizar ataques de gran capacidad, incluso que afecten la infraestructura crítica de los estados, pero a estos, debido a la normativa nacional e internacional, solo se les puede perseguir criminalmente.

REFLEXIONES FINALES

Ante la interrogante ¿Son aplicables la disuasión y la legítima defensa, como modalidades de empleo de los medios de la defensa en el dominio del ciberespacio?, en el presente artículo, después de efectuar un análisis respecto a la conceptualización de disuasión y legítima defensa, y contextualizarlo dentro del ámbito del ciberespacio, ha quedado de manifiesto que teóricamente es factible el aplicar una política digital disuasiva.

No obstante lo anterior, respecto a la implementación de una política digital disuasiva, se evidencian situaciones que lo dificultan. Entre ellas, es factible destacar dos problemáticas relevantes que deben tenerse en cuenta en su implementación:

a. La primera vinculada al desarrollo tecnológico. Para ejercer la disuasión en el ciberespacio, no basta con tener un desarrollo considerable en ciberarmas, sino que conlleva mantener altos estándares de ciberseguridad y ciberdefensa a nivel país (sector privado y público), enfocándose en la confianza, conocimiento-mutuo, sistemas robustos, redundantes y resilientes, a fin de provocar el efecto de evitar una acción por parte de una amenaza

potencial, a través de medidas de negación y reprimenda, ya que las capacidades propias son capaces de mitigarla.

b. La segunda del punto de vista normativo. Ante un ataque a través de esta dimensión se evidencia como muy complejo para los estados (o las víctimas en general) determinar el origen, la atribución de los ataques y las motivaciones que hay detrás, por tanto, no es posible determinar fácilmente contra qué o quién se pretende ejercer la política de disuasión digital, ya que si el ataque fuera de un Estado o comprobablemente vinculado a este, es posible catalogarlo como una agresión. Por otra parte, tendría un tratamiento diferente al ser ejecutado por un grupo atacante con otra motivación, el cual indefectiblemente concurre por la vía de la persecución criminal (a través del derecho interno o internacional según corresponda), independiente del impacto o daño causado.

Existen interrogantes que podrían orientar al desafío de posicionarse como Estado digitalmente disuasivo: ¿Se posee la infraestructura tecnológica suficiente para mitigar operaciones de las potenciales amenazas? ¿Es posible identificar de manera oportuna la atribución y motivación de mis amenazas?

Las respuestas a estas interrogantes, contrastadas con el nivel de desarrollo y coherencia de la estructura tecnológica y normativa imperantes, conforman las directrices fundamentales a la hora de prevenir, planificar y ejecutar la respuesta ante un ciberataque que afecte a un Estado.

En consecuencia, se podría aseverar -tal cual como en el ejercicio de la disuasión en el ambiente físico- que la disuasión en el ciberespacio es un desafío que involucra diferentes actores y de todos los ámbitos. Se estima que la solidez y modernidad de la infraestructura, de la normativa y de la vinculación intersectorial, generan el efecto sobre una ciberamenaza, para que esta desista de realizar una operación, porque los costos y riesgos de ejecutarla son más altos que sus beneficios.

Por otra parte, en el presente artículo se evidencia -respecto a la invocación de la legítima defensa (restrictiva)-, que el posibilitar el uso de las capacidades con

medidas de reprimenda en el ámbito de las ciberoperaciones, en la práctica es muy complejo pero no imposible si es que se tiene la capacidad de determinar con total certeza el origen, atribución y motivación.

Los casos presentados demostraron que ante la imposibilidad de determinar el origen, atribución y motivación del agresor, debieron utilizar herramientas de mitigación de la amenaza, fuera del ambiente del ciberespacio, a través de la diplomacia y de la comunicación estratégica. Estas herramientas se estiman que también formarían parte importante de la acción digital disuasiva y los efectos y coherencia de la misma. Lo recientemente descrito, no significa que los estados no deban tener cibercapacidades de negación ni reprimenda, sino que es complejo el argumentar en los parámetros de la legítima defensa su uso ofensivo ante un ciberataque.

De acuerdo a ello, además se podría establecer que la cooperación internacional, también forma parte (al igual que en la dimensión física) de las modalidades de empleo de los medios factibles de utilizar como parte de la disuasión y acciones de defensa, ante agresiones a través del ciberespacio.

REFERENCIAS

Arenas M. (2013) *Planificación de Fuerza y la Estrategia Marítima*. https://revistamarina.cl/revistas/2013/3/arenas.pdf

Asamblea General de las Naciones Unidas. (1974). *Resolución 3314*. Organización de las Naciones Unidas. https://www.acnur.org/fileadmin/Documentos/BDL/2007/5517.pdf?file=fileadmin/Documentos/BDL/2007/5517

BBC. (2015). *El virus que tomó el control de mil máquinas y les ordenó autodestruirse.* BBC News. https://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet

Bravo, C. (2017). *Apuntes de Ciberseguridad*. No publicado.

Chinchilla, M. (2018). *La efectividad de la teoría de la disuasión en la proliferación de armas nucleares en Oriente Medio*. Documento Marco, Instituto Español de Estudios Estratégicos. http://www.ieee.es/Galerias/fichero/docs_marco/2018/DIEEEM02-2018_Armas_Nucleares_MonicaChinchilla.pdf

Consejo de Seguridad. (2004). *Resolución 1540*. Naciones Unidas. https://undocs.org/sp/S/RES/1540(2004)

Diario Oficial. (9 de marzo del 2018). Ministerio de Defensa Nacional aprueba Política de Ciberdefensa. Número 42.003, Sección I, Ministerio del Interior y Seguridad Pública. http://www.diariooficial.interior.gob.cl/publicaciones/2018/03/09/42003/01/1363153.pdf

Gobierno de Chile. (2015). *Agenda Digital 2020: Chile digital para todos*. http://www.agendadigital.gob.cl/files/Agenda%20Digital%20Gobierno%20de%20Chile%20-%20Noviembre%202015.pdf

Gobierno de Chile. (2017). *Política Nacional de Ciberseguridad 2017-2022*. https://www.ciberseguridad.gob.cl/media/2017/05/PNCS-CHILE-FEA.pdf

Markoff, J. (2008). *Georgia sufre la guerra cibernética.* El País. https://elpais.com/diario/2008/08/14/internacional/1218664803_850215.html

McGuinness, D. (2017). *Cómo uno de los primeros ciberataques de origen ruso de la historia transformó a un país*. BBC Mundo. https://www.bbc.com/mundo/noticias 39800133#:~:text=Los%20estonios%20de%20habla%20rusa%20protestaron

Ministerio de Defensa Nacional. (2017) *Libro de la Defensa Nacional de Chile*. http://www.defensa.cl/media/LibroDefensa.pdf

Organización de las Naciones Unidas. (1945). *Carta de las Naciones Unidas*. http://www.un.org/es/charter-united-nations/

Información de Contacto

Academia de Guerra del Ejército / Centro de Estudios Estratégicos
Valenzuela Llanos 623 - Campo Militar La Reina
Fonos: 22 668 3415 - 22 668 3414
www.acague.cl / www.ceeag.cl