



La revolución tecnológica militar: Una mirada crítica¹

Resumen

Históricamente, la tecnología ha estado al servicio de la defensa y en consecuencia ha modificado el arte de hacer la guerra. De esta manera, el presente artículo analiza el desarrollo tecnológico para comprender la evolución de la guerra y su incidencia en el posicionamiento y la capacidad de los Estados en el Sistema Internacional, teniendo en cuenta además aspectos tan importantes como la economía y la geoestrategia. En consecuencia, resulta imperante tomar como eje de análisis a las Fuerzas Armadas como actores principales y decisivos en la revolución tecnológica de cara a las nuevas amenazas que aquejan a los Estados y que reconfiguran otros campos del poder nacional.

The Military technologic revolution: A critical look

Abstract

Historically, the technology has served to the Defense and as a consequence the Warfare is being modified. Thus, this article analyses the technological development to understand the war evolution and its incidence in the State's positioning and capacity into The International System, also taking into account economics and geostrategic aspects. Therefore, it is important to take The Armed Forces as a core of analysis and like principal and decisive actors in the technological revolution with a view to the new threats that afflict to the States and reshape other fields of the national power.

La aplicación de la tecnología al servicio del arte de la guerra ha sido inherente a la historia de la humanidad. Desde los primeros tiempos, el arco servía para el combate y la caza siendo así una tecnología de "doble uso" (Montoya, 2007), lo cual significa que la tecnología y la defensa

**HAYLYN ANDREA
HERNÁNDEZ FERNÁNDEZ²**

Recibido:
21 de octubre de 2015

Aprobado:
30 de noviembre de 2015

Palabras claves:
Tecnología, Innovación,
Seguridad, Fuerzas Armadas,
Defensa, Poder, Ciberseguridad.

Key words:
Technology, Innovation,
Security, Armed Forces,
Defense, Power, Cybersecurity.

1. Artículo de reflexión producto del proyecto de "Inteligencia Tecnológica", del grupo de investigación: "Centro en Investigación en Guerra Asimétrica -CIGA- adscrito y financiado por la Escuela de Inteligencia y Contrainteligencia "Brigadier General Ricardo Charry Solano".
2. Magister en Seguridad y Defensa Nacionales de la Escuela Superior de Guerra. Profesional en Relaciones Internacionales y Estudios Políticos de la Universidad Militar Nueva Granada. Asesora e Investigadora del Departamento de Educación, Ciencia, Tecnología y Doctrina de la Escuela de Inteligencia y Contrainteligencia "BG. Ricardo Charry Solano". Contacto: hahernandezf@gmail.com.

siempre se han articulado en función del bienestar de la población encausada principalmente en el ámbito militar.

En consecuencia, la evolución no se ha enmarcado solo al ámbito de los conflictos, sino también en el interés de los gobiernos de invertir en desarrollos tecnológicos tanto en los campos tradicionales como en estar a la vanguardia para combatir potenciales amenazas del terrorismo. Esto ha generado que la supremacía en la tecnología sea un factor preponderante y de impacto para la consecución de éxitos militares, en escenarios bélicos y previos a los mismos.

Además, no se desconoce que dadas las nuevas amenazas de la guerra bajo formas no convencionales (insurgencia, guerrilla, terrorismo), se necesita que el desarrollo de la ciencia y la tecnología vaya de la mano con el sector defensa para garantizar un ambiente libre de amenazas.

De esta manera, surge el interrogante de ¿Cuál es la importancia de la evolución de la tecnología militar para el sector defensa?, a través de la identificación de las principales tendencias tecnológicas y científicas de carácter militar se pretende responder a dicha pregunta.

Tal y como señala Van Creveld, quien dedica muchas de sus obras a estudios de los avances tecnológicos, es importante analizar la incidencia del desarrollo tecnológico y científico de carácter militar al unísono con el arte de la guerra, esto con el objetivo de comprender la complejidad de la evolución de la guerra de las últimas décadas.

En virtud de lo anterior, el presente artículo propone hacer una revisión panorámica de la tecnología aplicada al campo militar, para determinar la tecnología e innovación como factores decisivos a la hora de mantener el potencial y el posicionamiento de los Estados en el Sistema Internacional de cara a las nuevas amenazas que afectan la seguridad nacional. Para tal efecto, en primer término es necesario proyectar a la luz de la teoría de la Revolución en los Asuntos Militares algunas transformaciones que en el ámbito de lo militar generaron cambios tácticos y estratégicos gracias a los avances tecnológicos que marcaron la diferencia con el enemigo. Este análisis, permite hacer una trazabilidad entre

el la tecnología y la posición de los Estados traducido en términos de poder e influencia. En segunda instancia, se tienen en consideración factores de gran importancia como lo son la economía y la geoestrategia para ampliar el margen de análisis e incluir aspectos que protagonizan las nuevas dinámicas del sistema contemporáneo, en este escenario se resalta el gasto en defensa como un punto de partida para analizar el desarrollo y la capacidad de los Estados en el sistema internacional. De esta manera se genera un interrogante con respecto a lo que se conoce como “gasto” en defensa, concepto el cual es interpretado en la presente investigación como “inversión” en defensa por los beneficios que ello implica. Por último, proyectando la tecnología en el sector defensa, se destaca la importancia de la ciberseguridad y el intercambio de la información como criterios de particular atención por los retos y la vulnerabilidad que implican para la seguridad de los Estados, al respecto se esboza de manera general qué aspectos deberían incluir la Estrategia Nacional en Ciberseguridad.

Si bien la historia de la humanidad ha demostrado innumerables ejemplos de saltos tecnológicos de gran importancia; propiciados principalmente por los conflictos armados, es necesario ir más allá y visualizar su incidencia en escenarios futuros. La continua búsqueda de la seguridad implica que los Estados desarrollen y mejoren sus capacidades militares tanto defensivas como ofensivas de la mano con las ventajas y herramientas que proporciona la era de la globalización digital, pero esto no significa que la tecnología per se garantice la supremacía militar en cualquier tipo de conflicto. Ahora, siendo la mayoría de conflictos asimétricos, no se resuelven solo con tecnología, pero sin esta son difíciles de ganar. Se requiere de un ambiente integrado que combine herramienta propias de la ciencia, tecnología e innovación (García, 2001, p. 11).

En la medida en que las mejoras de las capacidades tecnológicas estén acompañadas de estrategias y políticas gubernamentales, se pueden aprovechar la diversificación del sistema a sectores civiles que combine tecnologías en pro de un entorno propicio para la innovación. Sin embargo, esto genera que en respuesta a la generación de desarrollo grupos paraestatales busquen emular e incluso superar las capacidades de defensa militar, lo cual implica un

“dilema de seguridad”³ influenciado por los desarrollos tecnológicos en el campo militar. Un clásico ejemplo es la carrera armamentística de la Guerra Fría entre la Unión Soviética y Estados Unidos, ya que enmarca la dinámica de acción-reacción entre poderes rivales (Buzan, 2008, p. 4).

Al respecto, cabe señalar que la evolución de la tecnología de las comunicaciones, fue determinante en el periodo de la Guerra Fría, impuso un nuevo punto de partida para el desarrollo de los conflictos ya que se habla de importantes avances (la comunicación satélite de órbita geoestacionaria, sistemas de multiplexado, transmisión de datos por conmutación de paquetes de información, comunicaciones de radio, guerra electrónica, sólo por mencionar algunos) que son muestra de nuevos métodos o tecnologías que se adaptan a diferentes formas de guerra no convencionales (Orti, 2007). Esto se da como resultado de una adaptación a las necesidades a las cuales responde la tecnología moderna.

De esta manera, la era de la globalización y la tecnología enmarcada en un sistema multipolar pone de manifiesto que las nuevas amenazas; que incluyen aspectos políticos, económicos, sociales, de salud y ambientales, exigen que las Fuerzas Armadas deben estar dotadas y capacitadas para enfrentar un escenario de guerra híbrida (ya que el número de conflictos de medio-bajo nivel irá en aumento y será más frecuente la intervención de grupos no estatales) que amenaza la estabilidad de la seguridad y defensa de los Estados, en consecuencia será el escenario propicio para que la ciencia y la tecnología estén a la vanguardia.

Con base en lo anterior, es necesario indicar que el concepto de “guerra híbrida” busca “fusionar la letalidad del conflicto estatal con el fervor salvaje y fanático de la guerra irregular, el término híbrido captura tanto su organización como sus medios” (Eissa, 2008, p. 2). Las guerras híbridas serían, según Frank Hoffman, las llamadas guerras irregulares, que serán cada vez más comunes, pero con “mayor velocidad y letalidad que en el pasado debido en parte a la difusión de la tecnología mili-

tar avanzada” (2009). Esto con el fin de clasificar o enmarcar la dinámica de los conflictos a los que se enfrentan los Estados en la actualidad.

Para ahondar en la relación de las apreciaciones anteriores con el concepto de tecnología es necesario hacer un análisis retrospectivo y establecer

De la Revolución en los Asuntos Militares

La cultura estratégica occidental intenta explicar el rápido cambio tecnológico y la revolución científico tecnológica a través de la teoría de la Revolución en los Asuntos Militares (-RMA- Revolution in the Military Affairs por sus siglas en inglés)⁴ en la década de los noventa; esta teoría apunta a que las transformaciones que se implementan en la estrategia militar no afectan los niveles social, político o económico.

El éxito de una contienda bélica depende de la fortaleza productiva y tecnológica de cada uno de los actores implicados en el conflicto. Este ha sido un patrón de pensamiento de particular éxito para Occidente, a causa de su fe en el desarrollo científico y condicionantes económicos, sociales (capitalismo y proceso de modernización) y políticos (la democracia)” (Molina, 2005, p 79).

La RAM es una revolución evolutiva-estratégica que está relacionada con la sociedad basada en la información y el conocimiento gestionados por las nuevas tecnologías, no es otra cosa que una teoría sobre el futuro de la guerra, generalmente relacionada con la tecnología y aspectos organizativos (Molina, 2005), en últimas la RAM acabó utilizándose para explicar los cambios en la tecnología, estructura, organización, tácticas militares y cambios doctrinales que han revolucionado la forma de combatir y garantizar la supremacía de los ejércitos que la han conquistado (Collom, 2014, p. 115).

Teniendo en cuenta las anteriores consideraciones, se puede inferir que se concibe a la RAM como la combinación de varias innovaciones en el seno de las Fuerzas Armadas, las cuales pueden encon-

3. “Se trataba de un concepto estructural que sostenía que los esfuerzos unilaterales de los estados para mantener su propia seguridad nacional, sean cuales sean sus intenciones, llevaban a un incremento de la inseguridad de los demás, dado que cada estado interpreta sus propias medidas como defensivas y las de los demás como potenciales amenazas” (Buzan, 2008, p. 4).

4. Es un concepto introducido a principios de la década de 1980 por Andrew W. Marshall, director de la Oficina de Net-Assessment del Pentágono. Marshall tuvo acceso a las reflexiones de los soviéticos y aceptó su punto de vista sobre el carácter potencialmente revolucionario de las nuevas tecnologías (Jordán, 2014).

trarse a lo largo de toda la historia en la medida en que la aparición de nuevas tecnologías modifique el arte de la guerra. Por ejemplo, durante la Primera Guerra Mundial se puso de manifiesto una de las grandes innovaciones militares procedentes de la revolución industrial del siglo XIX que tuvieron lugar durante las guerras napoleónicas. Las nuevas innovaciones serían la capacidad de movilizar y equipar a grandes ejércitos, de abastecerlos y trasladarlos por ferrocarril, coordinarlos mediante el teléfono y luego a través del telégrafo, y una capacidad de combate con enorme potencia de fuego gracias a los avances de la artillería y las armas de repetición. “A ello habría que añadir otras innovaciones asociadas a avances tecnológicos como el submarino, la aviación o el carro de combate” (Jordán, 2014).

Un caso representativo de la RMA producida durante la Segunda Guerra Mundial sería la Blitzkrieg alemana o Guerra Relámpago⁵. Superadas ya las guerras tradicionales al estilo napoleónico que generaba grandes desplazamientos de tropas que entraban en acción conforme a las necesidades tácticas y estratégicas, la intensión a partir de entonces era destruir al enemigo, restarle capacidad y margen operativo como se evidenció con el caso práctico de la Blitzkrieg alemana “Guerras cortas que necesitaban menos armas y mantenían el nivel de vida”. Esta táctica militar empleada en la Segunda Guerra Mundial implica inicialmente un bombardeo acompañado de uso de fuerzas móviles con velocidad y sorpresa para bloquear la capacidad de respuesta del enemigo.

Además, esta táctica prometía vencer, a través de la combinación de los vehículos blindados, infantería mecanizada, artillería y bombardeos; una rápida ofensiva sin desgaste. En últimas, la Guerra Relámpago, combinó nuevas tecnologías en armamento y comunicación que sumadas con el elemento sorpresa y concentración de fuerzas surtieron un efecto devastador.

Teniendo en cuenta que las definiciones entorno al concepto de la RAM son múltiples y polémicas; dependiendo de la visión de los profesionales de la

guerra, el factor que se debe rescatar al respecto es que se intenta explicar un periodo de transformaciones y el factor más nombrado como responsable directo de este cambio es la tecnología:

Tecnología en información, ordenadores, comunicaciones digitales y armas inteligentes, entre otras. Un avance que permitiría localizar rápidamente al enemigo, acceder a cualquier información necesaria en cualquier momento, poder comunicarla y actuar en consecuencia de la manera más rápida, precisa, letal y eficaz para la neutralización de la amenaza. (Benedicto, s.f.).

Ahora bien, es preciso señalar que para hablar de una RAM en un concepto amplio el uso o la aplicación de la tecnología necesita de factores adicionales que permitan un proceso más eficaz y decisivo. Son entonces los procedimientos operativos y la doctrina claves para que una RAM logre una transformación profunda en la concepción, organización y ejecución de una guerra. Todas estas acepciones al respecto van a modificar de forma directa la esencia de la naturaleza de la guerra, generando cambios de fondo que materialicen el cambio hacia una era posindustrial, posmoderna dominada por la información y la tecnología.

Si bien, se mencionaron someramente algunas de las llamadas RAM no es el objetivo del presente trabajo ahondar en su evolución e identificación exhaustiva a través de la historia, la intención por el contrario es evidenciar que el proceso de transformación de la información y la tecnología enmarcado en la era de la globalización redefine la forma de planear, hacer y conducir la guerra.

Los nuevos paradigmas tecnológicos aplicados a la naturaleza de la guerra ponen sobre la mesa el rol de los combatientes y en sí mismo la lógica organizacional de las Fuerzas Armadas, pero además supone un reto de más impacto ya que las implicaciones de la revolución al campo militar da paso al surgimiento de nuevos retos, problemas y realidades que obligan a los países a desarrollar estructuras defensivas más adecuadas. En este sentido, los cambios tecnológicos seguirán teniendo influencia y consecuencias en el ámbito de la defensa, razón por la cual las Fuerzas Armadas deben continuar

5. La táctica de Blitzkrieg fue desarrollada por el oficial del Ejército Alemán Heinz Guderian, cuyo axioma militar era: “Schlagen Sie hart und schnell”, “golpee duramente y rápido”. El objetivo era perforar y penetrar para luego destruir al enemigo desde la retaguardia con movimientos envolventes.

con un proceso de revisión y transformación, esto significa que, (i) deben ser capaces de generar valor añadido de la información y conocimiento; por lo cual no se debe desistir del concepto operativo, es decir, lo que a finales del siglo XX se conoció como RAM en todas las dimensiones (terrestre, naval, aérea, submarina, espacial, informacional, estratégica), y (ii) deben conducir y darle operatividad a las capacidades propias de las fuerzas de cara a la revolución tecnológica (Sanjuero, 2011, p. 48).

Un común denominador de las transformaciones vistas desde las RAM es que la tecnología ha incidido directamente sobre los cambios en la estructura de poder del sistema internacional. Basta con hacer una visión retrospectiva al periodo de la Guerra Fría que junto a con la Carrera Espacial fue una competición tecnológica que consolidó la era de la globalización e impulsó el surgimiento de un marco de relaciones internacionales bastante dinámico y complejo que reconfiguró la distribución del poder y generó la multiplicidad de actores en el sistema y la consolidación de un nuevo entorno de amenazas

Es entonces innegable la relación intrínseca entre la influencia de la transformación tecnológica, la connotación del poder y la posición estratégica de los Estados dentro del sistema internacional. Esto sugiere que es prioridad para cualquier nación disponer de capacidad tecnológica, no solo para tener influencia y una posición estratégica a nivel internacional, sino por un sentido básico de seguridad propio, dadas las nuevas tendencias y amenazas para las cuales deben estar preparados los mecanismos de defensa estatales, más exactamente las Fuerzas Armadas.

En consecuencia, el campo de batalla se adecua o se modifica de acuerdo a los nuevos sistemas de información que de cierta manera actúan como catalizadores estratégicos para disipar la “niebla de la guerra”. Ahora bien, esto implica que los cambios subyacentes a la era de la información demanden una combinación e integración de esfuerzos que sobrepasará las fronteras perceptibles hasta el momento; áreas tácticas (primeras líneas o de contacto), operacionales (espacio o zona de batalla) y estratégicas (retaguardia). Se habla entonces de un campo de batalla ausente de combatientes ya

que los ataques serían realizados a gran distancia por armas inteligentes y precisas, este es un campo propio de la era de la información: el ciberespacio, al respecto los nuevos conceptos militares deberán apuntar al incremento de actividades en ámbitos de la guerra y dominio de la información.

Las estrategias estratégicas y tácticas deberán versar entonces sobre el campo de batalla digitalizado asumiendo un rol de defensa ahora en el ciberespacio, es decir, la ciberdefensa⁶ a través de la implementación de doctrinas que orienten los procedimientos del uso de la tecnología como ventaja estratégica a la hora de conservar y mantener la posición en el sistema internacional salvaguardando la seguridad como fin esencial de cualquier Estado. El desarrollo de la relación de la ciberdefensa con la tecnología y su importancia para los Estados se tratará más adelante.

Reconfiguración del poder

Algunos referentes históricos que han sido objetos de análisis en la presente investigación han demostrado que la tecnología aplicada al sector defensa en cabeza de las Fuerzas Armadas han generado ventajas representativas, pero lo que hasta el momento no se ha tenido en cuenta es que existen diferentes factores que influyen en la implementación de dichas tecnologías y un factor de particular relevancia es la economía, y en particular la destinación de recursos económicos al Sector Defensa.

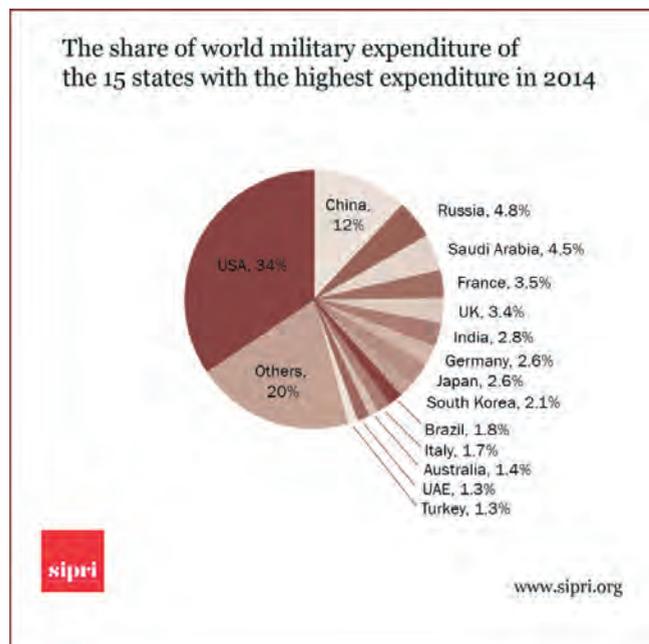
Teniendo en cuenta que la tecnología e innovación van a ser factores determinantes al momento de posicionar a los ganadores de la competencia internacional por mantener una posición estratégica; esto en cuanto al ámbito de la defensa, se debe hacer una trazabilidad más incluyente para tener en cuenta otros aspectos tan importantes como la economía y la geoestrategia. En ese sentido, el panorama actual evidencia que el centro de gravedad apunta al Asia Pacífico como una región pujante y en constante crecimiento, toda vez que sus economías representan el 55% del PIB mundial, llegando incluso a ser la región con el crecimiento más rápido en el mundo durante la última mitad del siglo

6. Capacidad del Estado para prevenir y contrarrestar toda amenaza o incidente de naturaleza cibernética que afecte la soberanía nacional.

(Friedman, 2010, p. 107). Alberga a dos de las mayores economías en el mundo, Japón y China, al igual que otras economías de importancia como lo son Taiwán y Corea del Sur.

Esta relación no se hace deliberadamente en el sentido que si bien esta zona está influyendo en el ámbito económico, también se caracteriza por tener una amplia influencia en el ámbito militar (campos que están estrechamente relacionados), basta con tener en cuenta la proporción del gasto militar a nivel mundial para comprender de manera general la relación de una economía pujante con el concepto de tecnología aplicado a la defensa.

Gráfico No. 1 Gasto militar mundial más alto en 2014.



Fuente: SIPRI. (2015). Stockholm International Peace Research Institute. Recent trends in military expenditure.

De acuerdo la gráfica anterior que representa datos obtenidos por el Stockholm International Peace Research Institute –SIPRI–, se hace una clasificación del gasto militar de los países, estas cifras son con relación al porcentaje del producto interno bruto (PIB) el cual se basan en datos del Fondo Monetario Internacional (FMI). De esta manera, Estados Unidos es el país con el gasto militar

más alto registrado para el 2014, de acuerdo con la base de datos del SIPRI, el porcentaje del gasto militar con respecto al PIB es del 3,8% y el porcentaje del nivel del gasto militar mundial corresponde al 34%. El liderazgo de Estados Unidos en materia de ciencia, tecnología e innovación será indiscutible en la primera mitad del siglo XXI. Pero esto sugiere que hay que poner especial atención a la región del Asia Pacífico.

China ocupa el segundo lugar a nivel mundial, tuvo un gasto militar mundial equivalente al 2,3% del PIB y una participación porcentual del gasto militar mundial del 12%. Se dice que China tendrá más impacto en el mundo en los próximos 20 años que cualquier otro país (Ramos, 2014, p. 14). Por otro lado se encuentran Japón y Corea del Sur representando al Asia Pacífico en el gasto militar mundial con el 2,6% y 2,1% respectivamente. Japón se sitúa en el puesto número 9 con el 1,0% del PIB y Corea del Sur en el número 10 con un porcentaje del 2,6 del PIB.

Si las tendencias actuales se mantienen en el tiempo, China deberá sortear los riesgos tecnológicos y medioambientales asociados a su desarrollo para llegar a ser incluso la primera economía a nivel mundial en el 2025 o por lo menos acortar sustancialmente la distancia con la economía norteamericana. En consecuencia, se potencializará como el mayor importador de recursos naturales y se convertirá en una potencia militar de primer nivel (Ramos, 2014, p.14).

En últimas, lo que se relacione con recursos representa prioridad en la agenda internacional de los países, se continuará generando una fuerte presión sobre el crecimiento económico mundial y el número de recursos de alto valor estratégico. En este sentido, se crea una simbiosis entre la capacidad militar, el peso económico y la tecnología (esto traducido en poder), factores que resaltan el papel de China como potencia industrial toda vez que combina el desarrollo económico y financiero-tecnológico en función de sus intereses, convirtiendo en epicentro de poder a Asia Pacífico. La sumatoria entonces del aspecto militar más la tecnología genera un aumento en las capacidades y una disminución significativa en las incertidumbres, en términos doctrinarios, reduce efectivos sin perder

operatividad transformando el carácter de los ejércitos (García, 2011).

Con base en el comportamiento de China, se debe tener en cuenta que basa su estrategia en sistemas de armas sofisticadas, pero de bajo coste, esto con el objetivo de mantener el control sobre sus aguas territoriales y hacer un contrapeso a las bases norteamericanas que rodean sus principales zonas de interés; los mares Oriental y Meridional de China. De esta manera y en contraste con Estados Unidos, China puede permitirse un crecimiento mucho más rápido de capacidad de despliegue y disuasión (Rodríguez, Turmo & Vara, 2013. p. 7).

Sin embargo, se debe tener en cuenta que el ejército chino está en conjunto poco desarrollado tecnológicamente, se basa actualmente más en número de soldados y de unidades que en armamento y sistemas de soporte (Rodríguez, Turmo & Vara, 2013. p. 19). Aun así, las universidades tecnológicas en China están creciendo lo cual genera que sea atraída buena parte de la juventud mejor formada, y por otro lado, el incremento del presupuesto militar chino apuntan a que la estrategia militar se redirija hacia proyectos militares en las tres áreas que impliquen uso intensivo de la tecnología de última generación. “Desde sistemas de comunicaciones hasta armamento convencional y no convencional, desde logística y organización hasta sistemas y programas de adiestramiento. En todas estas áreas, China tiene un amplio margen de mejora que puede aprovechar” (Rodríguez, Turmo & Vara, 2013. p. 19).

Tanto para el caso chino, como para los Estados que detentan el poder en el sistema internacional y de la mano con la revolución tecnológica global, se le debe apostar a la diversificación hacia sectores civiles para aprovechar la Innovación y Desarrollo (I+D) adquiridos en programas militares que se combinarían con la tecnología de otros sectores. Esto implicaría que se aumente la capacidad de una nación para transformar su potencial científico y tecnológico en ventaja competitiva de los mercados (Sanjuero, 2011, p. 38).

En materia de economía, ya que se necesitaría contar con el apoyo de empresas privadas o público-privadas, esto implicaría que el tipo de pro-

ductos que se generen tendrían un valor añadido y los salarios y demás remuneraciones que perciban los trabajadores serían más altos, razón por la cual afectaría positivamente a la población. Además, los conocimientos adquiridos de la tecnología militar serían transferidos a usos civiles de la tecnología, lo que implica el incremento del contenido tecnológico de los bienes y servicios en general (Rodríguez, Turmo & Vara, 2013. p. 19). En síntesis, el campo de la economía será uno de los más beneficiados por este tipo de programas que generan un proceso circular que siempre involucra tanto a la defensa como a la economía en beneficio del Estado.

Al término de estas modificaciones se espera que el gobierno chino reduzca los contingentes de las Fuerzas Armadas (reservas o fuerzas auxiliares) para destinar estos recursos, juntos con los derivados del incremento de la economía, a reforzar este tipo de programas. Las consecuencias para el campo militar serán las siguientes: (i) el desarrollo de tecnología militar inexistente en otros Estados y (ii) que las Fuerzas Armadas chinas incrementen y generalicen la tecnología de que disponen y sus unidades sean mucho más efectivas. La diferencia tecnológica entre las Fuerzas Armadas de Estados Unidos y China se reducirá, lo que genera la primera condición para variar el equilibrio de poder y centro de gravedad entre ambas potencias.

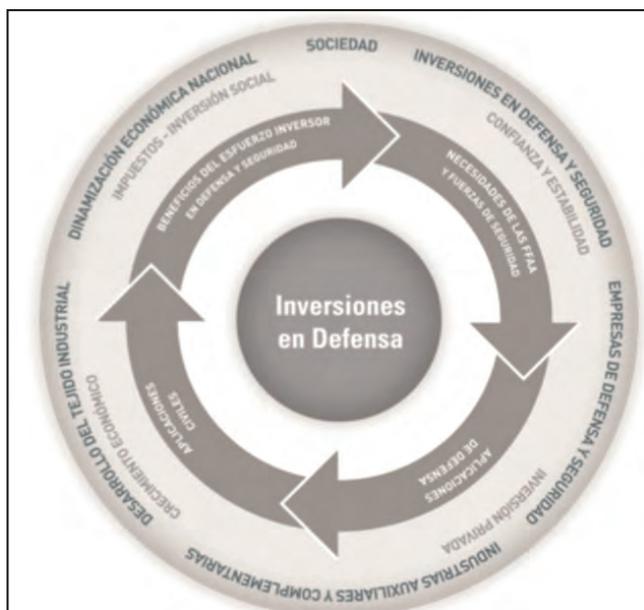
Ahora bien, el hecho de que se destaque el gasto en Defensa no es una condición fortuita, teniendo en cuenta los retos que deben enfrentar los Estados en los próximos años, esto implicará una inversión equivalente que permita mantener un estado libre de amenazas. Se habla entonces de potenciar la base industrial y tecnológica a través de esfuerzos de capacitación tecnológica que requieren inversiones tanto públicas como privadas (Ramos, 2014, p. 34).

En este sentido, es importante aclarar que en la última década la industria de la defensa no ha estado entre las diez primeras empresas del mundo por inversión en I+D, esto debido a que los departamentos de Defensa no disponen de los presupuestos necesarios para esta inyección de capital (García, 2011, p. 17). Por tal razón se habla de la necesidad de diversificar las actividades de la industria de la defensa, tanto en la seguridad interna

como externa hacia sectores civiles para aprovechar la I+D adquirida en programas militares que se combinaría con tecnología de otros sectores.

Es indispensable priorizar las garantías que genera el gasto en seguridad y defensa para un Estado ya que tiene un impacto positivo tanto en el campo económico como el social, entonces el gasto en defensa y seguridad corresponde más a una inversión. Al respecto:

Gráfico N° 2. Circulo virtuoso de las inversiones en Defensa.



Fuente: Ramos, C. (2014). El impacto de las nuevas tecnologías y las formas de hacer la guerra en el diseño de las Fuerzas Armadas del futuro. En Cuadernos de Seguridad Nacional, El impacto de las nuevas tecnologías y las formas de hacer la guerra en el diseño de las Fuerzas Armadas (pp. 13-36).

De acuerdo a las apreciaciones de César Ramos, Director General de la Asociación española de Empresas Tecnológicas de Defensa (TEDAE), con respecto al círculo virtuoso de las inversiones en Defensa, señala que ninguna economía, y por lo tanto ninguna sociedad, puede progresar sin un entorno seguro, estable y libre de amenazas. Las condiciones de seguridad garantizan un crecimiento económico sostenible ya que genera confianza para la inversión y el desarrollo (2014).

Por otro lado, sí se mantiene la inversión en seguridad se garantiza una herramienta para articu-

lar la capacitación tecnológica de un Estado. Esto teniendo en cuenta que ahora, los Estados no requieren de Ejércitos numerosos sino tecnológicos y operativos; la ola digital ha transformado los ejércitos. Incluso, se puede incluir el término de *Ejércitos Polivalentes*, es decir, capaces de responder a cualquier tipo de misión en tiempo de guerra o en tiempo de paz.

En la actualidad, el escenario estratégico con bajas probabilidades de conflicto armado incluye con mayor fuerza el impacto de amenazas transnacionales; hostilidad en el ciberespacio, riesgos de desastres naturales, protección de los recursos naturales, trata y tráfico de personas, proliferación y tráfico de armas de destrucción masiva –MDW-, falsificación de medicamentos, minería ilegal, tráfico de armas, lavado de activos y particularmente el narcotráfico, etc., amenazas que influyen en el deber ser de las Fuerzas Armadas las cuales deben ser reconfiguradas según criterios del siglo XXI.

De cara a los nuevos desafíos que impone el escenario mundial, las Fuerzas Armadas deben estar dotadas para enfrentar la guerra híbrida ya que irá en aumento el número de conflictos de bajo-medio nivel, en los cuales la intervención de grupos no estatales y el empleo de tecnología será decisivo, el escenario de ciencia y tecnología debe estar a la vanguardia en función del escenario en seguridad y defensa.

Por esta razón es que se puede deducir que la inversión en seguridad y defensa, ya sea en presencia de amenazas o en un ambiente relativamente seguro, aumenta el crecimiento económico de una sociedad.

Para mantener una posición estratégica en este siglo se necesitaría, por un lado, conseguir una ventaja tecnológico-científica que garantice un puesto relevante en el ranking económico a nivel mundial, y por el otro, mantener una capacidad militar que sea la consecuencia lógica de su desarrollo tecnológico, industrial y económico (Sanjuro, 2011, p. 48).

En este sentido, y como se mencionó anteriormente, la proliferación de conflictos de baja intensidad forzará a los Estados a intervenir en zonas

equidistantes de las fronteras tradicionales, las Fuerzas Armadas deberán enfrentarse a un abanico de armas de alta tecnología, es decir, se verán ampliadas las dimensiones del arte de la guerra.

En consecuencia, aparece un “nuevo lugar de batalla” propio de la era de la información, de la cual se desprende una nueva manera de entender y llevar a cabo la guerra,

[...] Nuevos conceptos militares abrirán paso a un incremento de actividades en determinados ámbitos: guerra de información, dominio de la información, campo de batalla vacío, campo de batalla digitalizado, enfoque sistémico del combate, operaciones sobre la información, etc. Las nuevas orientaciones estratégicas y tácticas se simularán, probarán y ensayarán en laboratorios y observatorios. (Benedicto, s.f., p. 34).

Aparece entonces un espacio que es la espina dorsal de la capacidad tecnológica, económica e industrial de este siglo; el ciberespacio.

La tecnología en el campo de batalla del siglo XXI

En la actualidad se han dado cambios en materia de las comunicaciones incitados principalmente por la necesidad de tener contacto permanente con el mundo exterior, además de la dependencia que se ha creado alrededor de la tecnología. De esta manera, la búsqueda permanente por lograr una comunicación eficiente y que abarque largas distancias, ha sido el génesis de grandes inventos que de una u otra forma han facilitado y cambiado el modo como hoy se comunican los seres humanos.

Es así, como se pasó del desarrollo de ruidos, expresiones y señales, a la transmisión de voz, video y datos a través de una red mundial de computadores llamada “internet”. En un primer momento, Internet se empleó con objetivos militares. Se diseñó como una red capaz de funcionar incluso en caso de que algunos de sus nodos fueran destruidos (ya que la información circularía por otros cauces de la red). Se habla del proyecto DARPA del

Pentágono, que consistía en tener una red informática que permitiera interconectar los computadores que comandaban los misiles estratégicos de Estados Unidos. Posteriormente, las universidades y las industrias se interesaron por esta red y fueron poco a poco cobrando protagonismo dentro de la misma. Actualmente Internet es un fenómeno social y económico que facilitó el proceso de comunicación y modificó la estructura social de la humanidad.

Para tener una definición más clara, internet es entendido como una red de ordenadores interconectados que permite un conjunto de servicios y aplicaciones de los cuales se puede hacer un uso provechoso. Este gran invento, considerado por muchos autores como uno de los más importantes de la humanidad, cambió la forma en que gran parte del mundo trabaja, se comunica e interactúa.

Existe una complejidad con respecto al poder de la computación, se deriva de la participación del ser humano en el sistema. El cambio tecnológico exponencial ha tornado el medio ambiente más complejo que nunca.

Aunque no era su objetivo inicial, la masificación de internet mutó hacia un área de tamaño inimaginable, con un alcance cada vez más extenso y más difícil de controlar. Esta área es “el ciberespacio”, definido por la NATO *Cooperative Cyber Defense Center of Excellence -CCDCOE-* como el ambiente formado por componentes tangibles e intangibles, caracterizado por el uso de computadoras y del espectro electromagnético, para almacenar, modificar e intercambiar datos usando redes de computadores.

Tras el avance de la tecnología, se puede inferir que la Tercera Revolución Industrial ha influido en nuevas manifestaciones de la guerra, estableciendo un nuevo campo del poder militar; el Ciberespacio (Gaitán, 2011, p. 23). Bajo este escenario, ha surgido una nueva tipología de enfrentamiento interestatal denominado como Ciberguerra, la cual busca paralizar o destruir las conexiones y las infraestructuras críticas de un país anulando sus sistemas informáticos (Instituto Español de Estudios Estratégicos, 2010, p. 16).

Ahora que la tecnología debe extenderse a otros campos de batalla, entre estos el ciberespacio por ser el objeto de estudio, se debe tener en cuenta que es precisamente allí donde radican las mayores vulnerabilidades de los Estados (Sanjuro, 2011, p. 46).

Las guerras han evolucionado a través de los años y sus armas también. La historia ha demostrado que las primeras guerras se lucharon con flechas y espadas, luego a cañones, rifles, bombas, misiles balísticos y armas inteligentes. Sea cual sea el tipo de arma que se haya usado, sus efectos y capacidades han estado limitadas a los cuatro dominios tradicionales de la guerra (tierra, mar, aire y espacio), los cuales se han definido por el tipo de tecnología militar desarrollada y utilizada hasta cada época.

La naturaleza de la guerra ha tenido varias transformaciones “los alcances tecnológicos abarcaron el desarrollo de las armas de fuego y la artillería, el poder se concibió como terrestre. Al desarrollarse la industria de guerra naval, surgió el poder marítimo. Con la llegada de las aeronaves se instauró el poder aéreo. Finalmente, posterior al advenimiento al espacio exterior de la Tierra se determinó el poder espacial” (Gaitán, 2011, p. 23). Es así que el ciberespacio fue señalado por *The Economist*, como el quinto dominio después de la tierra, el mar, el aire y el espacio.

Para efectos inmediatos, los Estados deben conducir y operativizar la capacidad de las Fuerzas Armadas de cara a la revolución digital con el objetivo de asegurar un espacio libre de amenaza, fortalecer e incrementar la ciberseguridad⁷.

A su vez los avances tecnológicos del mundo civil construyen y evolucionan el ciberespacio, impulsan la utilización masiva en el campo de batalla de las técnicas de digitalización y de las tecnologías de la información, facilitando la conectividad, es decir, se debe lograr un verdadero espacio de combate integrado virtual que formará el ciberespacio como un todo. De allí la importancia de la diversificación de hacia sectores civiles como se había enunciado anteriormente, ya que también la ciberseguridad se vería fortalecida.

Siendo que es un interés vital para todos los Estados garantizar el desarrollo económico, social y cultural, la protección del ciberespacio se consolida como un instrumento básico para lograr este fin, materializado a través del diseño e implementación de una Estrategia Nacional de Ciberseguridad. Estados Unidos se percató de esta necesidad en 1998, durante el segundo mandato de Bill Clinton, pero fue hasta el 2003 en la administración de George Bush cuando en Congreso norteamericano aprobó la Estrategia de Seguridad Nacional en el Ciberespacio. Alemania, desarrolló la estrategia Nacional de Ciberseguridad en el 2011 (Coz & Fojón, 2011, p. 82), España implementó la Estrategia de Ciberseguridad en el 2013 y así hay diferentes países como Canadá, Australia, Reino Unido, Holanda, Japón, entre otros que han gestionado la implementación de una Estrategia Nacional de Ciberseguridad. Sin embargo, hay otros países como Colombia que aún no disponen de una Estrategia Nacional, aunque han implementado diferentes mecanismos para la defensa del ciberespacio.

Para el caso particular de Colombia, el Consejo Nacional de Política Económica y Social del Departamento Nacional de Planeación, emitió en el 2011 el documento CONPES 3701, sobre los lineamientos de política para ciberseguridad y ciberdefensa con colaboración de otras instituciones involucradas como por ejemplo el Ministerio de Defensa, el Ministerio del Interior y el Ministerio de TIC'S. La problemática central que trata el documento se fundamenta en la capacidad actual del Estado para enfrentar las amenazas cibernéticas, presenta debilidades y señala que aún no existe una Estrategia Nacional de Ciberseguridad (CONPES, 2011, p. 2).

En la práctica, las Estrategias Nacionales de Ciberseguridad deberían basar su funcionamiento en unos ejes centrales, (i) Liderazgo del Estado en materia de ciberseguridad, (ii) La creación de una estructura organizada de control, (iii) Formación en torno a temas de ciberseguridad, (iv) Impulso económico público-privado, (v) Gestión de I+D sobre ciberseguridad y por último, (vi) Legislación y normalización de la ciberseguridad (Coz & Fojón, 2011, p. 82).

7. Capacidad del Estado para minimizar el nivel del riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética.

Para tal efecto es necesario que las estrategias estipulen metas bien definidas que vayan al unísono con los intereses nacionales de los Estados, además dentro de los objetivos que se tracen se debe diferenciar el rol de los sectores público y privado, ya que éste último va a soportar en gran medida la Estrategia de Ciberseguridad. Se necesita entonces la suma de esfuerzos para fortalecer y avanzar en una estrategia integradora que propenda por hacer de la Defensa una herramienta de cambio.

En cabeza del Sector Defensa se debe anticipar el uso de las tecnologías del futuro e innovar en su desarrollo a todos los sectores, desde los científicos y técnicos, hasta la industria y las Fuerzas Armadas (Pereira, 2011, p. 95). La intención de estas capacidades versa sobre la necesidad de que la defensa genere una ventaja competitiva de los futuros competidores, en ese sentido, la ciencia, tecnología e innovación son ejes que crean nuevas ventajas, pero además de eso se necesitan mejoras en el sistema de educación y renovación en el tejido científico-tecnológico de los Estados, es decir, inversión en la base industrial nacional; esto con el objetivo de reducir riesgos e incertidumbres en materia de defensa desarrollando capacidades militares.

Históricamente se ha demostrado que las naciones que han sabido adaptar, asimilar y gestionar las nuevas tecnologías, han tenido más éxito que las que se han mostrado más reacias a asumir innovaciones, las naciones deben apuntar a tener una capacidad para transformar su potencial científico-tecnológico en ventaja competitiva de los mercados.

Ahora bien, debido a que la tecnología ha ampliado el espacio de batalla (mar-tierra-aire), al espectro electromagnético y a las áreas del ciberespacio y el espacio exterior, se debe tener en cuenta que las estrategias reactivas por parte de los Estados no son suficientes para detener las amenazas. Mejorar el intercambio de información es fundamental para la detección de incidentes cibernéticos, no se consolida como una solución total pero es un paso crucial hacia las mejoras en Ciberseguridad.

Los beneficios del intercambio de información son numerosos, ya que permite a las organizaciones

mejorar sus defensas cibernéticas mediante el aprovechamiento de sus capacidades, el conocimiento y la experiencia de una comunidad más amplias (Zheng & Lewis, 2015, p. 1). En pocas palabras se habla de que el éxito del intercambio depende de las relaciones de confianza entre diferentes sectores, modelos de negocios compartidos y objetivos comunes.

Nuevamente se genera la sinergia productiva entre sector público y privado ahora desde el campo de la información, el intercambio de información sobre amenazas cibernéticas permite la fusión de una amplia comunidad involucrada e interesada que vela por un mismo fin ya que permite la consolidación de sus intereses. La finalidad del intercambio de información será reducir riesgos de manera colectiva, disuadir los ataques y mejorar la capacidad global, hasta el momento esta estrategia la ha implementado Estados Unidos, hoy en día, el intercambio de información sobre la amenaza cibernética entre las empresas privadas y con el gobierno es más estructurado, frecuente y regular. Sin embargo, aún hay varios retos legales y estructurales sobresalientes a la mejora de intercambio, como la preocupación por la privacidad, el riesgo de la responsabilidad y la función apropiada del Estado (Zheng & Lewis, 2015, p. 8).

Así las cosas, el ciberespacio como un nuevo dominio de la guerra desdibuja las fronteras y obliga a que los Estados; involucrando al ámbito civil y la seguridad militar, creen una estrategia integradora que se materialice a través de la innovación tecnológica para mantener las capacidades en defensa e industriales en el futuro, esto con el fin último de consolidar el poder militar como un factor importante a la hora de mantener una posición estratégica en el sistema internacional.

Resumiendo, la tecnología ha hecho evolucionar los conceptos del arte de la guerra y ha tendido que estar a la vanguardia de los requerimientos operacionales. Dichos avances tecnológicos han generado cambios a la hora de conducir la guerra y condicionan a los Estados de capacidades militares y económicas; en el campo militar, la tecnología aumenta las capacidades y reduce las incertidumbres (García, 2011, p.11).

Los cambios tecnológicos seguirán teniendo profundas consecuencias en el ámbito de la defensa, las Fuerzas Armadas se verán obligadas a continuar en una profunda revisión y transformación, aun así no deben desistir del concepto operativo, deben ser capaces de generar valor añadido de la información y del conocimiento con el objetivo de conducir sus capacidades de cara a la revolución digital.

Mantener la posición estratégica entonces dependerá de la combinación de factores estratégicos que aseguren a los Estados una armonía operacional en función de sus intereses. La economía en alineada con la Defensa genera una ventaja tecnológico-científica que permitirá a los Estados tener relevancia internacional y al respecto habrá que hacer un seguimiento minucioso, ya que si bien la ciencia y la tecnología actualmente se concentran sobretudo en Estados Unidos, Europa y Japón, el desplazamiento del poder y centro de gravedad económico hacia Asia Pacífico implican que la revolución tecnológica global será decisiva en esta parte del mundo.

Referencias

- Benedicto, R. (s.f.). Teorías y conceptos para entender formas actuales de hacer la guerra. Barcelona: Universidad Autónoma de Barcelona.
- Buzan, B. (2008). People, States & Fear: An Agenda for International Security Studies in the post-Cold War Era. *Revista Académica de Relaciones Internacionales*, (9), pp. 1-53.
- Collom, G. (2014). La revolución militar posindustrial*/The post-industrial military. *Revista de Estudios Sociales*, (50), pp. 113-126. Recuperado de <http://search.proquest.com/docview/1564372469?accountid=143348>
- CONPES. (2001). Política de manejo de Riesgo Contractual del Estado para Procesos de Participación Privada en Infraestructura. Recuperado de <http://portal.uexternado.edu.co/pdf/Derecho/Revista%20Digital%20de%20Derecho%20Administrativo/Jurisprudencia/CONPES-3107-RIESGO.pdf>
- Coz, J., & Fojón, E. (2011). Panorama internacional en el establecimiento de estrategias nacionales de ciberseguridad. *Estrategia*, pp. 82-83.
- Eissa, S. (11 de Octubre de 2007). Guerra híbrida: ¿una nueva forma de pensar la guerra en el siglo XXI? Recuperado de http://www.caei.com.ar/sites/default/files/working_paper_ndeg_36.pdf
- Friedman, G. (2010). Los próximos cien años. Barcelona: Destino, S.A.
- Gaitán, A. (2011). *Computadores e internet en la guerra interestatal: ¿la consolidación de un nuevo poder militar en el siglo XXI? Estudios en seguridad y defensa*, (6) 2, pp. 22-33.
- García, J. (2011). Panorama general de la tecnología y la industria de la seguridad y defensa. Instituto Español de Estudios Estratégicos -IEEE-, La innovación y la tecnología como factor estratégico diferenciador en el Siglo XXI. (pp. 13-22). Ministerio de Defensa.
- Hoffman, F. (2009). "Hybrid threats: reconceptualizing the evolving character of modern conflict. Strategic Forum, Institute for National Strategic Studies, National Defense University.
- Jordán, J. (2014). Innovación y Revolución en los Asuntos Militares: una perspectiva no convencional. Grupo de Estudios de Seguridad Internacional (International Security Studies Group). Recuperado de <http://www.seguridadinternacional.es/?q=es/content/innovaci%C3%B3n-y-revoluci%C3%B3n-en-los-asuntos-militares-una-perspectiva-no-convencional>
- Molina, D. (2005). *La Revolución de los Asuntos Militares (RAM) en el contexto de la era de la información*. *Revista de Estudios de Ciencias Sociales y Humanidades*, (14), pp. 77-85.
- Montoya, A. (2007). Tecnología y Fuerzas Armadas. Centro Superior de Estudios de la Defensa Nacional –CESEDEN-. Fundación Sagardoy.
- Ortí, J. (2007). Tecnología y Fuerzas Armadas (Antecedentes). Centro Superior de Estudios de la Defensa Nacional –CESEDEN-. Fundación Sagardoy.

- Pereira, M. (2011). La innovación y su implicación en el planeamiento de la defensa. En Instituto Español de Estudios Estratégicos -IEEE-, Panorama general de la tecnología y la industria de la seguridad y defensa (pp. 24-66). Ministerio de Defensa.
- Ramos, C. (2014). El impacto de las nuevas tecnologías y las formas de hacer la guerra en el diseño de las Fuerzas Armadas del futuro. En Cuadernos de Seguridad Nacional, El impacto de las nuevas tecnologías y las formas de hacer la guerra en el diseño de las Fuerzas Armadas (pp. 13-36).
- Rodriguez, Á., Turmo, J., & Vara, Ó. (2013). *El efecto de los desequilibrios económicos globales en la estrategia militar de los Estados Unidos y China*. Revista de Instituto Español de Estudios Estratégicos, (2), pp. 1-26.
- Sanjuro, J. (2011). La innovación y la tecnología como factor estratégico diferenciador en el Siglo XXI. Instituto Español de Estudios Estratégicos -IEEE-, La Defensa del Futuro: Innovación, Tecnología e Industria (pp. 23-66). Ministerio de Defensa.
- SIPRI. (2015). Stockholm International Peace Research Institute. Recent trends in military expenditure. Recuperado de <http://www.sipri.org/research/armaments/milex/recent-trends>
- Zheng, D., & Lewis, J. (2015). Cyber Threat Information Sharing. Recuperado de Center for Strategic International Studies -CSIS-: http://csis.org/files/publication/150310_cyberthreatinfosharing.pdf

ESCUELA SUPERIOR DE GUERRA



REPÚBLICA DE COLOMBIA

CEESEDEN

Estudios en

SEGURIDAD Y DEFENSA

Volumen 10 No. 20 diciembre de 2015

Para solicitar un ejemplar en físico o en formato PDF o para confirmar el acuse de recibo de la revista, por favor escribir a:

Escuela Superior de Guerra
Centro de Estudios Estratégicos sobre Seguridad y Defensa Nacionales
CEESEDEN

Carrera 11 No. 102-50 Teléfono: 620 40 66 Ext.:21455
e-mail: revistaceeseden@esdegue.mil.co
www.esdegue.mil.co

Bogotá - Colombia

MAESTRÍA EN ESTRATEGIA Y GEOPOLÍTICA

Registro Calificado Res. MEN 02869 de 2015. Cód. SNIES 104278



Fundada en 1909

Unión, Proyección, Liderazgo



ESCUELA SUPERIOR DE GUERRA

Carrera 11 No. 102-50. Of. 327, Bogotá

Conmutador: 620 40 66 Extensión 21067 - 20618

Teléfono Directo 629 49 90

