TRANSFORMACIÓN MILITAR

ISSN: 2590-664X

EDICIÓN 4. ABRIL 2020 **BOGOTÁ D.C.,** COLOMBIA

WWW.EJERCITO.MIL.CO

EJÉRCITO NACIONAL
PATRIA HONOR LEALTAD

2020 FORTALECIMIENTO DE LA PROFESIONALIZACIÓN MILITAR Y COHESIÓN DE LA FUERZA

EJC

COTEF

Fotografía:Ejército Nacional de Colombia

Military Transformation Journal: It is a professional analysis Journal published by the Colombian Army, the Transformation Command and its Strategic Analysis Center (CAEEF, for its Spanish acronym). It aims to present analysis, strategic and academic studies that may contribute to the decision-making process of the Colombian Army Transformation Command. The opinions expressed in this Journal do not necessarily represent the policies or points of view of this Center, nor of any other Unit of the Colombian Army.

SUMARIO

Transformación Militar: Es una revista profesional de difusión y análisis publicada por el Ejército Nacional, a través del Comando de Transformación Ejército del Futuro y su Centro de Análisis Estratégico Ejército del Futuro (CAEEF), que tiene como fin producir análisis y estudios estratégicos y académicos que contribuyan al proceso de toma de decisión del Comando de Transformación del Ejército y la difusión del conocimiento fuera y dentro de la Institución. Las opiniones expresadas en esta Revista no necesariamente representan las políticas o puntos de vista de este Centro ni de alguna otra dependencia del Ejército Nacional.

ISSN: 2590-664X
Edición 2020 Abril

EDITORIAL

2020, Centro de Análisis Estratégico Ejército del Futuro (CAEEF)

Calle 102 N° 7 – 80 – Teléfono: 571 – 7470680, extensión 107
Bogotá D.C., Colombia.

AGRADECIMIENTOS ESPECIALES

A los miembros del Comité Editorial por su invaluable labor como pares evaluadores de los artículos.

A los miembros de la oficina de enlaces internacionales: al Señor Coronel (r) Luis Sánchez Aldana , al Coronel Luciano Barcellos da Cunha del Ejército de Brasil y al Coronel Ricardo Olivos Reyno del Ejército de Chile, por su apoyo en el fortalecimiento de los enlaces de comunicación con otros países.

Al Profesor Antônio Eustáquio Lino, maestro en idiomas de la Universidad Militar Nueva Granada de Colombia, por su apoyo en la traducción de los artículos.

A la Sargento Primero Piedad Olaya Gutiérrez y a la Oficina de Comunicaciones Estratégicas del COTEF, quienes brindaron sus más distinguidos aportes en todas las etapas de publicación.

Fotografía:Ejército Nacional de Colombia

Eduardo Enrique Zapateiro Altamiranda

Mayor General
Comandante del Ejército Nacional

Nació el 18 de julio de 1962 en la ciudad de Cartagena, departamento de Bolívar. Ingresó a la Escuela Militar de Cadetes «General José María Córdova» en el año de 1983 y ascendió como Subteniente del arma de Infantería en el año de 1985. El 30 de diciembre de 2019 fue designado como Comandante del Ejército Nacional por el Presidente de la República, Dr. Iván Duque Márquez.

La transformación que el Ejército Nacional inició hace una década es el motor que ha impulsado la implementación de una nueva estrategia, dinamizando nuestras capacidades para atender los retos del presente y afrontar las amenazas futuras en el campo de la seguridad y defensa de la nación.

En este contexto, el Ejército Nacional tiene como objetivo fundamental continuar desarrollando el pensamiento estratégico de sus hombres y mujeres, para que interactúen con las diversas autoridades gubernamentales y demás organismos del Estado, con el propósito de transitar del control militar al control institucional del territorio.

Este proceso de transformación también ha generado el interés de distintos sectores académicos, tanques de pensamiento y universidades a nivel nacional e internacional, quienes a través de su visión vienen aportando insumos académicos a la evolución de los procesos que adelanta actualmente el Ejército en materia de estrategia de seguridad y defensa nacional, políticas y directrices, y por ende, los planes estratégicos que se desarrollan en el nivel operacional y táctico.

Bajo esta óptica, el Ejército Nacional y el Comando de Transformación Ejército del Futuro (COTEF) ha consolidado, a través de la Revista *Transformación Militar,* una red académica e interdisciplinar de expertos e investigadores a nivel nacional e internacional en temas relacionados a la modernización y optimización de procesos militares, estudios de caso de transformación en otros ejércitos del mundo, y el análisis de nuevas amenazas y factores de inestabilidad, para que a través de escritos puedan compartir a los lectores sus conceptos y experiencias

En esta cuarta edición de la Revista *Transformación Militar,* el Ejército de la República Federativa de Brasil, con un grupo de investigadores de sus centros de pensamiento, participa con importantes artículos que exponen los avances de esa institución frente a temas que son de común interés para la seguridad fronteriza y la misionalidad de los ejércitos de Brasil y de Colombia.

También se destaca la participación de importantes académicos e investigadores de amplia trayectoria, que compartieron de manera puntual sus experiencias

en las reformas al sector seguridad en Kosovo y Túnez. En temas propios de seguridad nacional como los que tienen que ver con la minería ilegal en el departamento de Chocó, las amenazas del ciberterrorismo y los desafíos que enfrenta el Ejército colombiano ante el surgimiento de la guerra híbrida, la revista presenta el análisis de observadores e investigadores nacionales que nos ayudan a visionar la magnitud de estos.

Por último, resaltamos la participación de agencias gubernamentales para la cooperación internacional y el desarrollo y de estudios estratégicos en defensa como el Institute for Defense Analysis y la Folke Bernadotte Academy, quienes aportaron escritos sobre la reforma al sector seguridad desde una perspectiva de género y de Planeación Basada en Capacidades en ambientes complejos y cambiantes.

Es válido en esta edición agradecer al mando anterior y a todos aquellos que brindaron sus más distinguidos aportes en la publicación de esta revista que presento como un medio de interacción para el desarrollo del pensamiento estratégico de la institución con la academia, el análisis y la investigación.

Teniendo en cuenta el alto valor académico con el que cuenta la Revista *Transformación Militar,* y reconociendo la importancia que esta tiene para seguir fortaleciendo el diálogo permanente entre el Ejército y todos los sectores de la sociedad, invito al público lector a ser parte de este encuentro académico de significativo interés para el Sector Seguridad y Defensa y la transformacion del Ejército Nacional de Colombia.

"EL EJÉRCITO NACIONAL TIENE COMO OBJETIVO FUNDAMENTAL CONTINUAR DESARROLLANDO EL PENSAMIENTO ESTRATÉGICO DE SUS HOMBRES Y MUJERES, PARA QUE INTERACTÚEN CON LAS DIVERSAS AUTORIDADES GUBERNAMENTALES Y DEMÁS ORGANISMOS DEL ESTADO".

Robinson Alexander Ramírez Cedeño

Mayor General

Jefe de la Jefatura de Estado Mayor de Planeación y Políticas
Ejército Nacional de Colombia

Profesional en ciencias militares, economista con más de 30 años de experiencia liderando procesos de planeación estratégica, comando y control, transformación institucional, operaciones de logística, así como procesos de Educación y Doctrina en el Ejército Nacional de Colombia.

El Comando de Transformación Ejército del Futuro (COTEF), fiel a su compromiso con las políticas del Comando del Ejército, lanza un nuevo número de la Revista *Transformación Militar* que da cuenta de su compromiso con la investigación y de producción de análisis para el desarrollo del pensamiento estratégico de la Fuerza. Lo anterior a partir del desarrollo de líneas estratégicas enfocadas hacia el estudio de distintas experiencias nacionales e internacionales de transformación, reformas al sector seguridad y procesos de modernización y optimización de procesos al interior de instituciones militares.

El desarrollo de estas líneas se construyen en respuesta a los intereses actuales de la Fuerzas Militares, pero también con base a la transversalización de las áreas funcionales de la transformación, comprendidos en el estudio de tendencias, escenarios, capacidades y prospectiva en el marco de la transformación, para así poder reflexionar sobre los retos y desafíos que el Ejército colombiano necesita enfrentar en relación con el contexto de seguridad que caracteriza el ambiente operacional actual.

Para ello, la cuarta edición de T*ransformación Militar* contó con el aporte de expertos analistas e investigadores de corte nacional e internacional que encaminaron sus esfuerzos a analizar nuevos escenarios de seguridad, así como experiencias mundiales de reformas al sector seguridad, haciendo un énfasis especial en los procesos de modernización y optimización de procesos que permitan hacer frente a nuevos contextos de seguridad en los que surgen actores irregulares con capacidad de desestabilizar el orden nacional e internacional, por medio de la combinación de métodos tradicionales y no tradicionales.

"EL COTEF (...) LANZA UN NUEVO NÚMERO DE LA REVISTA TRANSFORMACIÓN MILITAR QUE DA CUENTA DE SU COMPROMISO CON LA INVESTIGACIÓN Y DE PRODUCCIÓN DE ANÁLISIS PARA EL DESARROLLO DEL PENSAMIENTO ESTRATÉGICO DE LA FUERZA".

El nivel de profundidad de análisis, así como la participación de autores, agencias gubernamentales y centros de pensamiento con el más alto nivel académico, le permite a la Revista *Transformación Militar* establecerse como una ventana a través de la cual el Ejército de Colombia evidencia sus avances en materia de transformación, pero también por medio de la cual la Fuerza está al tanto de los esfuerzos que otros ejércitos del mundo vienen desarrollando en materia de transformación militar. El alto valor académico con el que cuenta la revista, sumado a sus características de innovación y vanguardismo, constituye a *Transformación Militar* como un insumo importante para seguir aportando con contundencia a la evolución y transformación de nuestro glorioso Ejército Nacional.

Juan Pablo Guzmán Torres

Coordinador editorial de la Revista Transformación Militar

Actualmente se desempeña como investigador asesor del Centro de Análisis Estratégico Ejército del Futuro (CAEEF), donde coordina la Revista Transformación Militar y apoya las demás iniciativas investigativas del Centro frente al papel del Ejército en escenarios de postconflicto, procesos de transformación en instituciones militares y el fortalecimiento de relaciones cívico-militares.

NOTA EDITORIAL
REVISTA TRANSFORMACIÓN MILITAR 2020

Por mandato constitucional, y por la complejidad de las realidades geográficas y de seguridad en las fronteras terrestres de Colombia, el Ejército Nacional asume roles propios de su naturaleza; es decir, salvaguardar la defensa y seguridad de la nación. No obstante, el surgimiento de nuevas amenazas, la evolución del crimen organizado trasnacional, la porosidad en zonas de frontera, así como las crisis migratorias, económicas y políticas que se han gestado en países vecinos, demandan que esta Institución se encamine a consolidar un ejército desarrollista que esté en la vocación de diversificar su capacidad de respuesta, aún cuando esto implique crear una nueva óptica operacional, sustentada en el desarrollo de acciones no armadas y asistencia militar.

Ante la posible intensificación de los fenómenos anteriormente mencionados, se hace cada vez más necesario identificar iniciativas, planes, marcos doctrinarios y límites de intervención del Ejército, a fin de articularlos de manera efectiva con las demás instituciones del Estado. Para ello, se considera fundamental trabajar sobre las oportunidades de mejora en torno a la articulación de la Fuerza con la oferta estatal y la consolidación del control institucional de un territorio que aún sigue presentando espacios vacíos de poder y la expansión de grupos armados sustentados en el empoderamiento territorial, la explotación de recursos de distinta naturaleza y la transnacionalización de las economías ilegales.

Comparto la afirmación del Profesor Eduardo Pizarro (2018), autor del libro *De la guerra a la paz: Las fuerzas militares entre 1996 y 2018,* cuando establece que "el caso de Colombia es en gran medida excepcional, en tanto la 'vieja' guerra revolucionaria que se había extendido por toda América Latina tras el triunfo del Movimiento 26 de Julio en Cuba en 1959, ha sabido (…) imbricarse con la 'nueva guerra', impulsada por organizaciones criminales globalizadas, portadoras de un extenso portafolio criminal". Aún cuando existen matices conceptuales y ambigüedades a la hora de catalogar estratégica y militarmente a estos nuevos grupos, puede decirse en primera instancia que los categorizados Grupos Armados Organizados y Grupos Delincuenciales Organizados[1] ya no son entendidos solamente como componentes militares o brazos armados de una estructura política, si no como organizaciones y bandas armadas al servicio de los poderes mafiosos de orden nacional e internacional, cuyas lógicas de operación se caracterizan principalmente por la ambivalencia y la capacidad de adaptación y re adaptación a las dinámicas territoriales y socioeconómicas de las regiones. [2]

A la anterior afirmación, me atrevería a agregar que esta nueva oleada de violencia armada y no armada responde, sin duda, a una coyuntura de postacuerdo que trajo consigo nuevos elementos políticos, sociales y económicos, en la que la cooptación de la población en los territorios sigue siendo un elemento esencial para obtener control territorial y legitimar el uso de la violencia directa y estructural.

Estas nuevas dinámicas de convergencia entre el acercamiento a las bases populares y comunitarias junto con la intimidación a la población civil demandan al Ejército repensarse y emprender una transformación institucional que tenga como objetivo ampliar su legitimidad institucional en los territorios, a través de una defensa activa, pero, ante todo, mediante acciones que contribuyan al desarrollo, capaces de consolidar un liderazgo regional integrador. En un contexto de seguridad en los que se resaltan los incesantes desplazamientos; las intimidaciones y amenazas contra reclamantes de tierras, representantes y líderes de organizaciones de población desplazada y víctimas; el reclutamiento de menores y la crisis migratoria, le compete al Ejército, más que nunca, establecer puentes de comunicación entre la población civil y las autoridades locales, en aras de fortalecer la gobernabilidad en los territorios y pasar del control militar al control institucional del territorio.

Bajo esta óptica, y con base en dichas necesidades, la Revista Transformación Militar se erige como una publicación que procura aportar a la construcción de ese contexto estratégico que permita al Ejército Nacional ampliar su visión respecto a los factores de inestabilidad, pero también frente a la creación de estrategias basadas en la modernización institucional y el desarrollo de capacidades. Gracias a la más distinguida colaboración de expertos y analistas de la seguridad y la defensa se ha logrado desde el año 2016 contar con artículos académicos dedicados a estudiar los cambios que han sufrido los

[1] Esta categorización se dio a partir de la Directiva permanente No. 15 expedida por el Ministerio de Defensa en el año 2016.

[2] Estas nuevas redes de criminalidad pueden considerarse como una amenaza multifacética, dedicada principalmente al comercio de drogas ilícitas, la extracción ilícita de yacimientos mineros, la extorsión y el tráfico ilegal, sin un aparente contenido ideológico o político, a excepción del ELN.

teatros de operación, así como las nuevas características que adoptan las guerras asimétricas y el estudio de procesos de transformación y reformas al sector seguridad a nivel mundial en coyunturas de posguerra y/o posconflicto. Estos aportes a su vez han logrado hacer de Transformación Militar una plataforma mediante la cual el Ejército ha fortalecido un diálogo permanente con la academia y la sociedad civil, al abrir sus canales de participación y convocatoria para que estudiosos de distintas disciplinas puedan aportar de forma actualizada al debate de seguridad en Colombia.

No sin antes agradecer a todos los autores que participaron en la elaboración de este número, a los miembros del Comité Editorial por su invaluable labor como pares evaluadores de los artículos, así como a los Señores Coroneles Luciano Barcellos da Cunha del Ejército de Brasil, Ricardo Olivos Reyno del Ejército de Chile, al Coronel (r) Luis Sánchez Aldana y a todos los integrantes del Comando de Transformación (COTEF) que brindaron sus más distinguidos aportes en todas las etapas de publicación, invito al público lector a hacer un repaso de los aportes académicos que componen esta cuarta edición de la Revista, a fin de seguir perpetuando el diálogo académico entre las instituciones militares y la sociedad civil, y seguir fortaleciendo el carácter multidisciplinario del Proceso de Transformación del Ejército, que se constituye como un bastión fundamental de la línea evolutiva del Ejército Nacional de Colombia.

REFERENCIAS

Pizarro, E. (2018). *De la guerra a la paz. Las Fuerzas Militares entre 1996 y 2018.* Bogotá: Editorial Planeta.

Fotografía:Ejército Nacional de Colombia

"LA REVISTA TRANSFORMACIÓN MILITAR SE ERIGE COMO UNA PUBLICACIÓN QUE PROCURA APORTAR A LA CONSTRUCCIÓN DE ESE CONTEXTO ESTRATÉGICO QUE PERMITA AL EJÉRCITO NACIONAL AMPLIAR SU VISIÓN RESPECTO A LOS FACTORES DE INESTABILIDAD, PERO TAMBIÉN FRENTE A LA CREACIÓN DE ESTRATEGIAS BASADAS EN LA MODERNIZACIÓN INSTITUCIONAL Y EL DESARROLLO DE CAPACIDADES".

Fotografía:Ejército Nacional de Colombia

EDITORIAL NOTE
MILITARY TRANSFORMATION JOURNAL 2020

Based on the normative framework, and the complexity of the security and geographical context of Colombia, the Colombian Army undertakes roles of its nature; that is, to defend the territorial integrity and sovereignty. However, the emergence of new threats, the evolution of transnational organized crime, the porosity in border areas, as well as the migratory, economic and political crises that have arisen in neighboring countries, demand that this institution moves towards the consolidation of a humanist and developmentalist army, whose participation emphasizes on the possibility of diversifying its response capacity, even when this implies creating a new operational perspective, based on the development of non-armed actions and military assistance.

Faced with the possible intensification of the aforementioned phenomena, it becomes increasingly necessary to identify initiatives, plans, doctrinal frameworks and limits to the Army's intervention, in order to coordinate them with other State institutions effectively. Given this, it is considered essential to work on opportunities for improvement around the coordination of the Force with the state supply and the consolidation of institutional control of a territory that still continues struggling with spaces empty of power and expansion of armed groups supported by the territorial empowerment, the exploitation of resources of different nature and the internationalization of illegal economies.

I share the statement of Professor Eduardo Pizarro (2018) in his book *De la guerra a la paz: Las fuerzas militares entre 1996 y 2018* when he considers that "the Colombian case is largely exceptional, as long as the 'old' revolutionary war that had spread throughout Latin America after July 26 Movement's triumph in Cuba in 1959, has managed to (…) coalesce with the 'new war', driven by globalized criminal organizations, carriers of an extensive criminal portfolio"[1]. Even though there are conceptual nuances and ambiguities when it comes to strategically and militarily cataloging these new groups, it can be said in first instance that Organized Armed Groups and Organized Crime Groups[2] are no longer understood as military components or armed structures of a political organization, if not as organizations and armed bands at the service of mafia powers of national and international order, whose logics of operation are characterized mainly by ambivalence and the ability to adapt and re-adapt to the territorial and socioeconomic dynamics of the regions.[3]

To the previous Pizarro's statement, I would venture to add that this new armed and non-armed violence wave responds, without a doubt, to a post-agreement situation that brought new political, social and economic elements with it, in which the cooptation of population in the territories continues to be an essential element to obtain territorial control in order to legitimize the use of direct and structural violence. As a result of the foregoing, it is possible to show that the spaces previously occupied by the former Revolutionary Armed Forces of Colombia (FARC, for its Spanish acronym) have become focal points for new actors, but also territorial bastions for the new composition of other armed groups that existed before the signing

[1] This citation was freely translated by the Editorial Note's author.

[2] This denomination was given to these organizations based on the Permanent Directive No. 15, issued by the Ministry of Defense in 2016.

[3] These new criminal networks can be considered as a multifaceted threat, dedicated mainly to the illicit drug trade, the illegal extraction of mining deposits, extortion and illegal trafficking, without an apparent ideological or political content, with the exempt of the National Liberation Army (ELN, for its Spanish acronym).

of the peace agreement: self-defense organizations and the Residual Organized Armed Groups (GAOr, for its Spanish acronym) better known as the dissidence of the FARC. These new dynamics of convergence between the approach to the popular and community bases, and the intimidation of the civil population, demands the Army to rethink and undertake an institutional transformation that is aimed to expand its institutional legitimacy in the territories, through an active defense , but, above all, through actions that contribute to the country's development, capable of consolidating an integrating regional leadership.

In a security context in which instability factors -such as incessant displacements, intimidation and threats against land claimants, the recruitment of minors and the migration crisis- exceeds the capacity of the state, it is the responsibility of the Army, more now than ever, to establish communication bridges between local communities and civil authorities, in order to strengthen the institutional capacity and governance in the territories, as a means to generate spaces to empower community leaders and local civil authorities.

Based on the above, the Military Transformation Journal stands as a publication that seeks to contribute to the construction of a strategic context that allows the Colombian Army to expand its vision regarding instability factors, but also to propel the creation of strategies based on institutional modernization and the development of capabilities to respond to present and future threats. Thanks to the most distinguished collaboration of security and defense experts and analysts, since 2016 the Journal has relied upon academic articles devoted to study the changes that asymmetric warfare and theaters of war have adopted, together with the study of worldwide security sector reform experiences in postwar and/or post-conflict scenarios. These contributions in turn have succeeded in establishing Military Transformation as a platform through which the Army has strengthened a permanent dialogue with the academy and civil society, by opening its channels of participation to scholars from different disciplines who want to contribute in an updated manner to the security debate in Colombia.

Not before giving the greatest recognition to all the authors who made part of this edition, the Editoral Committee members for their invaluable work as peer evaluators, as well as Colonel Luciano Barcellos da Cunha from the Brazilian Army, Colonel Ricardo Olivos Reyno from the Chilean Army and Colonel (r) Luis Sánchez Aldana for their indispensable contribution, and all the members of the Transformation Command (COTEF, for its Spanish acronym) who provided their most distinguished contributions in all stages of the publishing process, I invite the public to review the academic contributions that make up this fourth edition of the Journal, in order to continue with the academic dialogue between military institutions and the civil society, as well as the strengthening of the multidisciplinary nature of the Transformation Process, which constitutes a fundamental bastion of the evolutionary line of the Colombian Army.

REFERENCES

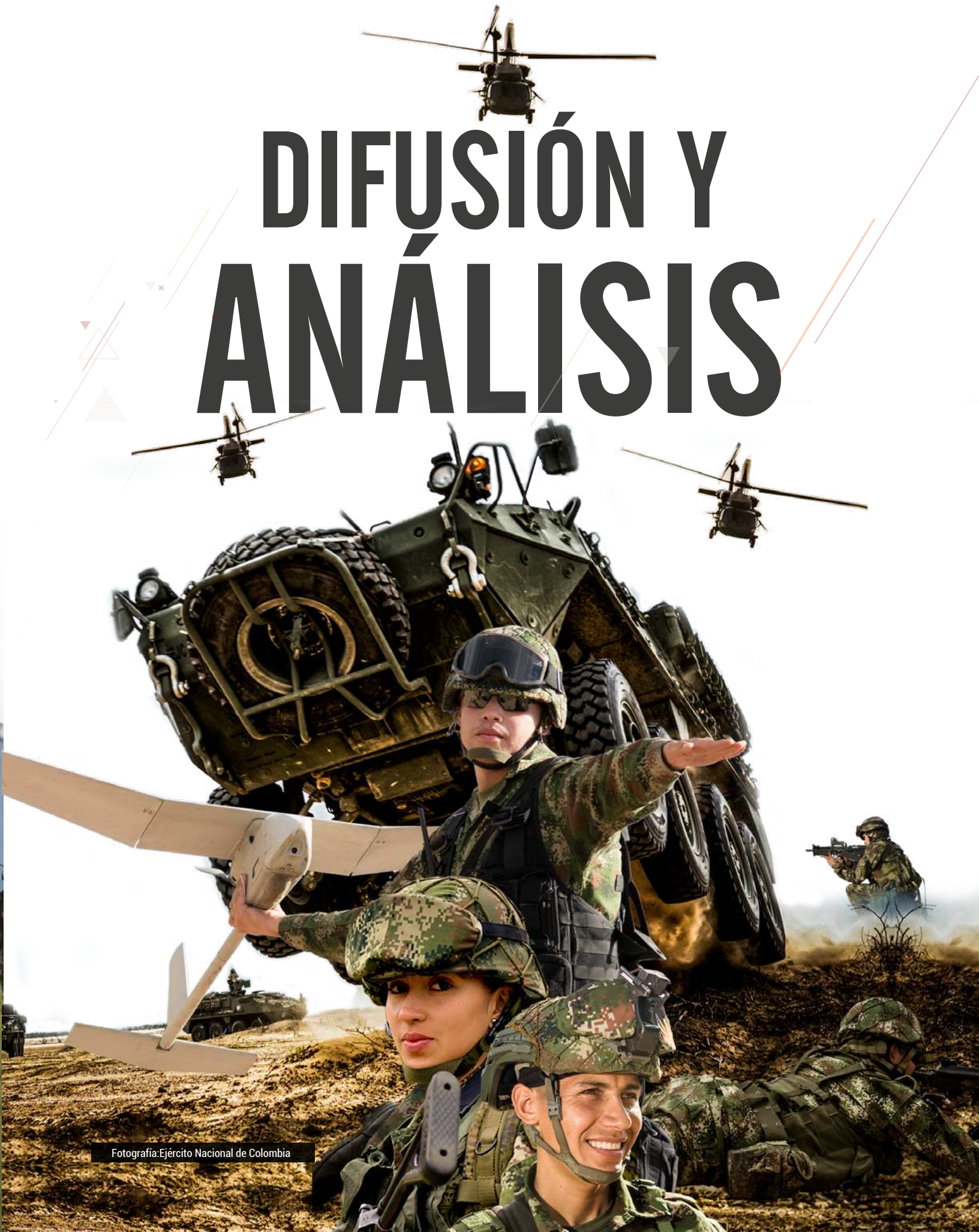
Pizarro, E. (2018). *De la guerra a la paz. Las Fuerzas Militares entre 1996 y 2018.* Bogotá: Editorial Planeta.

Fotografía:Ejército Nacional de Colombia

"THE MILITARY TRANSFORMATION JOURNAL STANDS AS A PUBLICATION THAT, THROUGH ITS THEMATIC LINES, SEEKS TO CONTRIBUTE TO THE CONSTRUCTION OF A STRATEGIC CONTEXT THAT ALLOWS THE COLOMBIAN ARMY TO EXPAND ITS VISION REGARDING THE INSTABILITY FACTORS, BUT ALSO TO PROPEL THE CREATION OF STRATEGIES BASED ON INSTITUTIONAL MODERNIZATION AND THE DEVELOPMENT OF CAPABILITIES TO RESPOND TO PRESENT AND FUTURE THREATS".

Fotografía:Ejército Nacional de Colombia

DIFUSIÓN Y ANÁLISIS



Fotografía:Ejército Nacional de Colombia

LAS CIBERGUERRAS Y EL CIBERTERRORISMO: ¿LOS NUEVOS TEATROS DE LAS GUERRAS?

Jaime Cimadevilla

Historiador e investigador sobre conflictos contemporáneos, relaciones internacionales y terrorismo. Asesor del Comando General de las Fuerzas Militares.

RESUMEN

La internet es una herramienta que ha facilitado el intercambio de información, obtención de productos y ampliación de los medios de comunicación por dar unos ejemplos. Sin embargo, también ha permitido la expansión de la guerra y el terrorismo a medios digitales. El artículo contempla de manera general las principales características, particularidades y desafíos que representan los nuevos teatros estratégicos, tácticos y operacionales tanto para las agencias y/o instituciones del Estado como para grupos armados insurgentes, criminales o terroristas. Así pues, el ciberespacio ha permitido infiltrar, sabotear y destruir infraestructura crítica de varios Estados gracias a las redes digitales que conectan todo un sistema de seguridad, lo que termina siendo un problema general para toda la sociedad: dependencia a la tecnología y, por lo tanto, ser extremadamente vulnerables ante una serie de ataques capaces de afectar toda la estructura comunicacional, económica y militar de un Estado. No obstante, las ciberamenazas o los ciberataques todavía están en un proceso de gestación porque sus capacidades militares no han sido por ahora capaces de sentenciar un ataque donde se afecten un considerado número de personas y se limita a compartir propaganda con el objetivo de perturbar la percepción de algún tema a la población civil. Por otra parte, es un tema necesario que hay que analizar y profundizar porque las tecnologías digitales avanzan cada día más rápido y están volviéndose parte fundamental de la cotidianidad de los grandes centros urbanos.

Palabras clave: *Internet, ciberespacio, terrorismo, tecnología, Estado.*

ABSTRACT

The Internet is a tool that has facilitated the exchange of information, the obtention of products and media expansion, by giving some examples. However, it has also allowed the expansion of war and terrorism to digital media. The article covers in a general way the main characteristics, the particularities and the challenges that represent the new strategic, tactical and operational principles for the agencies as well as for the insurgent, criminal or terrorist armed groups. Thus, cyberspace has allowed to infiltrate, sabotage and destroy the infrastructure of several states thanks to the digital networks that connect an entire security system, which ends up being a general problem for the whole society: dependence on technology and, therefore, being extremely vulnerable to a series of attacks. However, cyber threats or cyber attacks are still a gestation process, because their military capabilities have not yet been able to sentence an attack that affects a considerate number of people and is limited to sharing propaganda that aims to disturb the perception of the civil population on regards to a certain topic. On the other hand, it is a necessary issue that must be analyzed and deepened because digital technologies are advancing faster and faster and are becoming a fundamental part of the everyday life of cities and urban centers.

Keywords: *Internet, cyberspace, terrorism, technology, State.*

INTRODUCCIÓN

Las guerras han sido un fenómeno constante en la historia de la humanidad: desde las grandes batallas entre Estados hasta el levantamiento de movimientos insurgentes y grupos terroristas en conflictos interestatales, la violencia ha abierto su propio camino y ha sido aplicada de diversas maneras en distintos lugares del mundo. Sin embargo, los avances tecnológicos han desarrollado nuevos escenarios bélicos que generan numerosos tipos de daños que se apartan de los agravios de los rifles, los tanques, los aviones o los buques de guerra. Desde principios de los años noventa, la internet y las tecnologías digitales han progresivamente 'revolucionado los sectores del comercio, las comunicaciones, las acciones militares y la gobernanza' al punto de ser una herramienta útil para la conducción de la guerra, de actos criminales u actos terroristas (Knake, 2010).

Por eso, es necesario hoy en día hablar de las ciberguerras y el ciberterrorismo, ya que presentan escenarios dinámicos que se apartan de los campos de batalla convencionales. En estos contextos, la guerra no es solamente entre Estados o grupos irregulares. Es decir, uno o un grupo de hackers capacitados pueden robar información y/o filtrar un virus que puede afectar las finanzas de un banco, la seguridad de un individuo o la infraestructura crítica de un Estado. Es así que surge una de las particularidades de estos nuevos fenómenos: atacar sin la necesidad de grandes costos, porque no se necesita mantener con bastas cantidades alimentos o conservar adecuadamente la calidad de los equipos de una unidad militar, de una autodefensa, una guerrilla o una organización terrorista. Igualmente, las pérdidas son mínimas, porque los costos de una excelente computadora frente a los de una base militar, un portaviones o movilizar a una gran cantidad de soldados no inquieta severamente el presupuesto del Estado o una organización armada. El presente artículo es una breve introducción del tema de ciberguerras y ciberterrorismo: un análisis histórico que examina estas problemáticas y cómo han sido abordadas desde distintas perspectivas que van desde agencias de seguridad hasta académicos.

EL GIGANTESCO ESPECTRO DE LA ACTIVIDAD EN LA INTERNET

Primero, tenemos que revisar un par de terminologías para entender qué se entiende como ciberguerras y ciberterrorismo. La definición más básica de ciberguerra sería esta: 'Acciones de un estado-nación para penetrar las computadoras o redes de otra nación con el propósito de causar daño o interrupción' (Clarke, 2010, citado por Caplan 2013, Pág. 94). Por otra parte, la Oficina Federal de Investigaciones de EE.UU (FBI) define al ciberterrorismo como: 'Ataques premeditados y de motivación política contra la información, los sistemas informáticos, los programas informáticos y los datos que dan lugar a la violencia contra blancos no combatientes por grupos subnacionales o agentes clandestinos' (Gordon, 2002, 4). Como podemos apreciar, el concepto y su definición carece de una interpretación universal porque cada actor dependiendo de su orientación ideológica y cultural (sea un Estado, una organización terrorista o una organización civil por nombrar algunos ejemplos) construirá su propia definición sobre el tema.

Asimismo, las ciberguerras se comprenden como "guerras sin sangre" (Gray, 1997), cuyo fin no es neutralizar al enemigo físicamente, sino robar, sabotear o rastrear la información sin que el enemigo se entere. Sería una maniobra que Sun Tzu aplaudiría, porque no se encara al adversario directamente sino por arte del engaño. Podría decirse que son las guerras democráticas ideales porque no mueren ni soldados ni civiles por causas directas o por daños colaterales. Además, los daños colaterales y los costos de operación se ven notoriamente reducidos (Rid, 2013). Sin embargo, estas afirmaciones pueden verse superadas por la definición de ciberterrorismo elaborada por la profesora de informática del Naval Postgraduate School de los Estados Unidos, Dorothy Denning donde acierta que un ciberataque tiene que crear un impacto físico o muerte al afectar la infraestructura critica (Denning, 2000).

En el caso de internet o ciberespacio, puede estimarse que hay miles de millones de usuarios que emplean esta herramienta para leer noticias e informarse sobre

"APROXIMADAMENTE TRES MIL MILLONES DE PERSONAS USARON INTERNET EN 2017, **ES DECIR, APROXIMADAMENTE EL 48%** DE LA POBLACIÓN TOTAL MUNDIAL. PARA EL AÑO 2019, SE ESTIMÓ QUE EL **56% DE LOS HABITANTES DEL PLANETA TUVIERA ACCESO A INTERNET."**

lo que esté ocurriendo en el planeta en tiempo real. Según cifras proporcionadas por el Banco Mundial, aproximadamente tres mil millones de personas usaron internet en 2017, es decir, aproximadamente el 48% de la población total mundial. Para el año 2019, se estimó que el 56% de los habitantes del planeta tuviera acceso a internet. Asimismo, se especula que el gasto mundial en la Internet de las cosas (IoT) alcance los $ 745 mil millones en 2019, un aumento del 15,4% con respecto a los $ 646 mil millones gastados en 2018, según una nueva actualización semi anual del Internet de la Corporación Internacional de Datos (IDC, 2019), transformándose en una de las principales herramientas para el movimiento de las economías tanto nacionales como internacionales.

De esta manera, las redes de información y de conocimiento están compuestas por miles de millones de personas lo que hace que la internet sea el mayor archivo de información del planeta, haciendo arduo el seguimiento a un tema o concepto en particular. Estos son algunos de los desafíos que las ciberguerras han postulado a las agencias de seguridad de todo el mundo y deben replantearse varias políticas y visiones sobre como entonces ha evolucionado la guerra.

Otro punto inquietante de este fenómeno es con la velocidad que los avances tecnológicos se están haciendo. Por ello, en cuestión de años, una forma de conocimiento tecnológico y científico puede verse superado y volverse obsoleto. El profesor Paul Virilio llama "teoría de la cultura hipermoderna" a su "modelo de la guerra", el cual, explica que el flujo de la información se ha acelerado al punto que se consigue con mayor facilidad ante los avances tecnológicos proporcionados por la ciencia en el siglo XX. Lo increíble es que Paul Virilio describió este escenario en su libro Speed and Politics en 1977, casi una década antes de la creación del Protocolo de Puerta de Enlace de Frontera (BGP en inglés) y el PSINet (uno de los primeros proveedores de servicio de internet) en 1989, las cuales pueden considerarse como los puntos cardenales de la apertura comercial del internet (Tanenbaum, 2003, 459). Anteriormente, el conocimiento e información sobre la amenaza es lo que más tardaba en obtenerse. En la guerra, es vital obtener información para cuadrar operaciones, tener conocimiento de los números y operaciones del enemigo.

Fotografía:Ejército Nacional de Colombia

Un hacker puede iniciar un ataque desde su propio hogar y no desde una base militar o una agencia de seguridad como suponen las lógicas tradicionales de la guerra. Conjuntamente, el trabajo puede ejecutarse con pequeñas células en vez de grandes estructuras militares como una brigada o una división de las Fuerzas Militares.

Por lo tanto, una gran característica de este nuevo fenómeno es el cambio de la lógica de la guerra: se tratan de ataques descentralizados que son perpetuados desde distintas partes del planeta. Por ejemplo, un hacker puede iniciar un ataque desde su propio hogar y no desde una base militar o una agencia de seguridad como suponen las lógicas tradicionales de la guerra. Conjuntamente, el trabajo puede ejecutarse con pequeñas células en vez de grandes estructuras militares como una brigada o una división de las Fuerzas Militares. También, su alcance puede ser transnacional porque pueden infectarse con un virus o robarse información como lo hace grupos de "hackactivistas" como lo es Anonymous, conocidos por emplear la máscara de Guy Fawkes del comic V de Vendetta, tanto para esconder sus identidades como para propagar su agenda política a distintas partes del globo.

Esta guerra cibernética puede verse todos los días en una página de internet llamada Northstand, que parece a primera vista un videojuego, pero, en realidad, son ataques cibernéticos en tiempo real perpetrados por hackers con distintas alineaciones y diversos propósitos: organizaciones criminales, "hackactivistas", organizaciones terroristas, agentes independientes e incluso empleados de seguridad de algún Estado. No obstante, a pesar de estas revelaciones, ninguno de los países involucrados ha declarado abiertamente una guerra. Esto puede deberse, como acierta la investigación del profesor Thomas Rid (2013), a que este tipo de acción no desencadena una guerra convencional porque va en la misma línea de las técnicas del espionaje, cosa que está permitida dentro de los marcos tradicionales de las guerras o son actos criminales donde las Fuerzas Militares no tienen jurisdicción porque se trataban de robos a bancos o robos de información, situación que por lo general le corresponde a la jurisdicción a la Policía.

Fotografía:Ejército Nacional de Colombia

"WIKILEAKS LE EXPUSO AL MUNDO ENTERO QUE **EXISTÍA UNA GUERRACIBERNÉTICA** ENTRE CHINA, ESTADOS UNIDOS Y RUSIA: ATAQUE CON VIRUS, **INFORMACIÓN FALSA** SIENDO ENVIADA PARA CONFUNDIR AL ADVERSARIO E INTENTOS DE ROBO DE CONOCIMIENTO CLASIFICADO POR PARTE DE **HACKERS (SEAN DEL ESTADO O SEAN CONTRATADOS COMO TERCEROS** PARA DESVINCULAR CUALQUIER GOBIERNO, ORGANIZACIÓN TERRORISTA O MOVIMIENTO SOCIAL DE CUALQUIER ERROR)."

Las ciberguerras y el ciberterrorismo se han vuelto métodos alternativos para combatir la guerra. Por eso, los cables expuestos por Wikileaks y las filtraciones de información clasificada de la Agencia Central de Inteligencia (CIA) hechas por Edward Snowden, demostraron la vulnerabilidad y vacíos que tenían las agencias de seguridad del Estado ante sus estándares de seguridad informática. Por ejemplo, Wikileaks le expuso al mundo entero que existía una guerracibernética entre China, Estados Unidos y Rusia: ataque con virus, información falsa siendo enviada para confundir al adversario e intentos de robo de conocimiento clasificado por parte de hackers (sean del Estado o sean contratados como terceros para desvincular cualquier gobierno, organización terrorista o movimiento social de cualquier error). Un ejemplo de esto fueron los ataques cibernéticos hechos entre Irán, Israel y Estados Unidos, cuando estos dos últimos atacaron un centro de investigación nuclear en Natanz con un virus cibernético llamado "Stuxnet", el cual afecto la infraestructura critica del país persa. Por ello, uno de los nombres que se le ha dado a este fenómeno es "guerra suave" (Price, 2012).

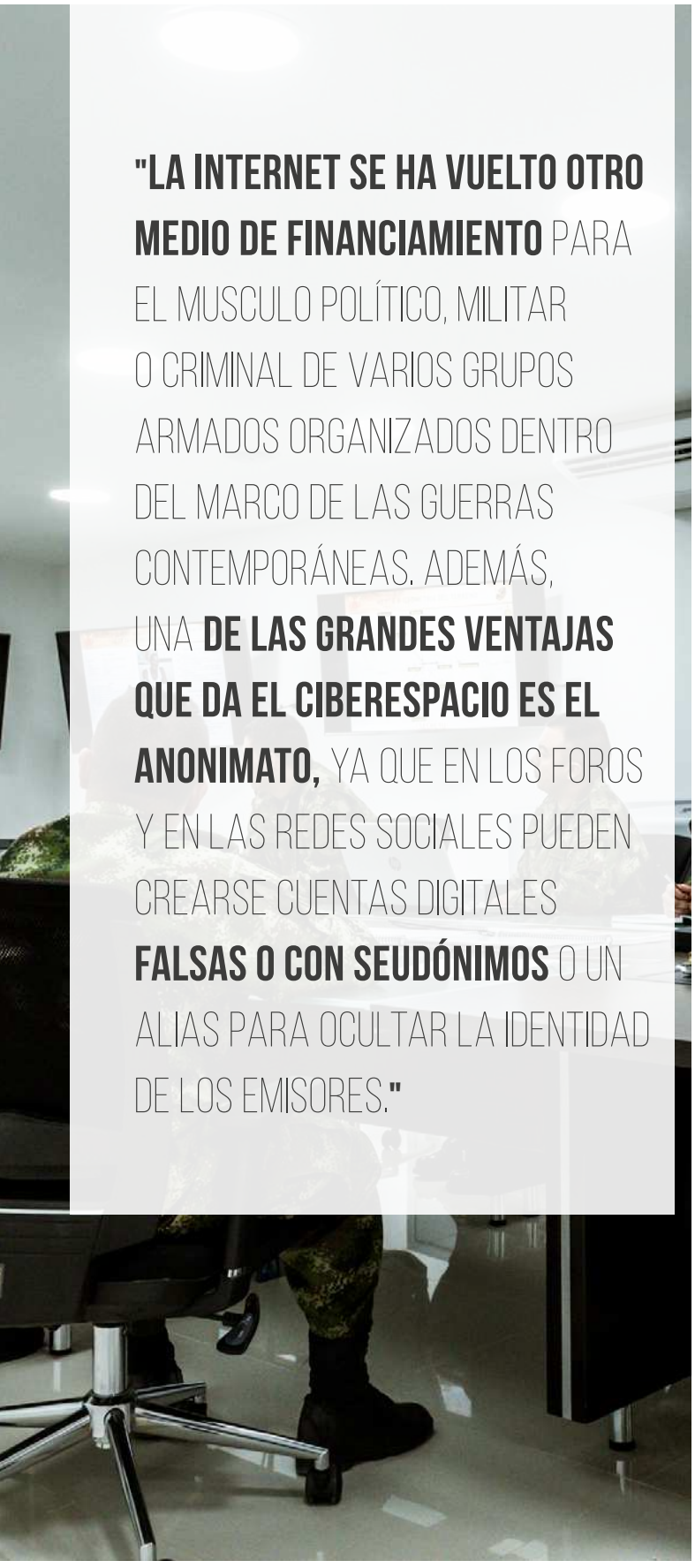
Este tipo de ataques también nos hacen replantear el concepto de "infraestructura critica"; ya no se trata de edificios o infraestructuras sino de datos e información que se encuentran en el plano digital: la vulnerabilidad de la información personal (tarjetas de crédito y/o dirección domiciliaria) y/o con grados de clasificación (confidencial, secreto o ultrasecreto) que es almacenada en bases digitales se encuentra en riesgo.

En ese sentido, las computadoras o los discos duros son clasificados como infraestructura física. Igualmente, hay que tener en cuenta que la gran mayoría de esta infraestructura funciona actualmente por medios electrónicos y digitales. Por lo tanto, si anteriormente se hizo el comentario de la bomba atómica, solo imagínense si tiene la capacidad de sabotear una represa, una planta energética o un hospital con el objetivo de afectar la cotidianidad de la ciudadanía.

En otras palabras, los grandes centros urbanos, donde se encuentra gran parte de la población y se concentra gran parte de los recursos económicos, se ha vuelto dependiente de la tecnología y, por lo tanto, extremadamente vulnerable a un ataque cibernético. Entonces, la formulación de estrategias alternativas que logren proteger la infraestructura tanto civil como militar va a ser uno de los temas centrales para las futuras generaciones como bien sentencian 'Para cada método inteligente y herramienta en desarrollo para ocultar información en datos de multimedia, un igual número de métodos inteligentes y de herramientas están siendo desarrollados para detectar y revelar sus secretos' (Wang. H, Wang, S., 2004, 76).

Por ello, organizaciones criminales o terroristas mueven millones de productos y de dineros por este medio. El más notorio ejemplo de esto es la "Web Profunda" (Deep Web) donde se trafican armas, drogas, contratación de sicarios, personas y otros productos en lo que sería la forma más innovadora y contemporánea de lo que coloquialmente se le suele llamar "mercado negro". También, de acuerdo con el Observatorio Europeo de Drogas y Toxicomanías (OEDT), delincuencia organizada y su financiación, varios grupos armados organizados han adoptado la "criptomoneda" o bitcoin para hacer transacciones tanto en el plano ilegal como legal con el fin de generar grandes ganancias en un nuevo sector económico (Pastor Gómez, 2017, 3) aparte de los métodos convencionales como el narcotráfico, tráfico de personas o el tráfico de armas. En otras palabras, la internet se ha vuelto otro medio de financiamiento para el músculo político, militar o criminal de varios grupos armados organizados dentro del marco de las guerras contemporáneas. Además, una de las grandes ventajas que da el ciberespacio es el anonimato, ya que en los foros y en las redes sociales pueden crearse cuentas digitales falsas o con seudónimos o

Fotografía:Ejército Nacional de Colombia



"LA INTERNET SE HA VUELTO OTRO MEDIO DE FINANCIAMIENTO PARA EL MUSCULO POLÍTICO, MILITAR O CRIMINAL DE VARIOS GRUPOS ARMADOS ORGANIZADOS DENTRO DEL MARCO DE LAS GUERRAS CONTEMPORÁNEAS. ADEMÁS, UNA **DE LAS GRANDES VENTAJAS QUE DA EL CIBERESPACIO ES EL ANONIMATO,** YA QUE EN LOS FOROS Y EN LAS REDES SOCIALES PUEDEN CREARSE CUENTAS DIGITALES **FALSAS O CON SEUDÓNIMOS** O UN ALIAS PARA OCULTAR LA IDENTIDAD DE LOS EMISORES."

un alias para ocultar la identidad de los emisores.

EL ROL DE LOS MEDIOS DE COMUNICACIÓN Y LAS REDES SOCIALES

Cabe recordar que el flujo de información en las redes sociales se ha vuelto un arma propagandista versátil y barata. Si nos ponemos a estudiar las funciones de los medios de comunicación, estos pueden abrir la puerta a la propagación de propaganda e información para influir en las actitudes políticas de las personas y sus creencias sobre el mundo en el que viven. Seguidamente, plataformas como Instagram, Facebook y Twitter han posibilitado el "astroturfing": es una técnica de marketing que consiste en ocultar la identidad del emisor de una propaganda electoral o los anuncios comerciales que pretenden dar una impresión de espontaneidad, como nacida de una fuerte relación con el entorno social. Esto es importante, porque marca las tendencias políticas y electorales de los emisores y productores de los medios de comunicación. En el caso colombiano, esta maniobra se ve claramente en la invasión de propaganda y desinformación en las redes sociales con el objetivo de atraer potenciales electores o forjar una conciencia colectiva que se oponga a un grupo o a un individuo. Como lo hacen algunos partidos políticos o grupos como Anonymous que desean generar un estado de paranoia con temas conspirativos para que haya una desconfianza o rechazo contra una facción. En otras palabras, crear un enemigo y así generar un sentido de identidad ideológica.

Seguidamente, hay que considerar la desinformación como una estrategia común en estos escenarios: información falsa o alterada con la finalidad de confundir al adversario o manipular con facilidad a los receptores, quienes en este caso son la población civil. Esta divulgación puede alterar la cosmovisión de una sociedad, en especial, si esta no es crítica del origen y veracidad de la información que llega a miles de dispositivos digitales (computadores, celulares, tablets por nombrar los más comunes). Igualmente, existen los perfiles falsos que son creados con dos fines: primero, proteger la identidad del emisor; segundo, crear una cadena de información difícil de rastrear en las densas redes digitales.

CONCLUSIONES

Las ciberguerras y el ciberterrorismo continúan con los mismos objetivos que los terroristas tradicionales, pero con diferentes medios. La internet ha brindado una alternativa para que las guerras y la criminalidad se extiendan a nuevos escenarios. Al ser temas tan recientes y cuyo impacto es difícil de medir, las ciberguerras y el ciberterrorismo no se le han marcado limites teóricos o prácticos. La internet pasó de ser una comodidad a una necesidad para la gran mayoría de habitantes donde exista un fácil acceso a la web. Así que esto puede permear todos los escenarios de la cotidianidad, al tocar diferentes espacios y contextos creados por los seres humanos.

Hay que resaltar que el fenómeno de la guerra cada vez es más denso y difícil de identificar. Esta situación hace que los objetivos, los procedimientos e incluso la identidad de las amenazas adquieran una identidad "híbrida": es el contexto en el cual los combatientes combinan sus estrategias y formas de operar con el objetivo de fortalecerse. Por ejemplo, la incursión de grupos armados con una ideología se une con grupos criminales que tienen la capacidad de transformarse y adaptarse a los nuevos escenarios con el fin de sobrevivir (Cimadevilla, 2019). También, este concepto abarca la posibilidad de ampliar el campo de batalla a nuevos escenarios: mantener la lucha armada convencional y combinarla con ataques cibernéticos como lo ha intentado el Estado Islámico (ISIS) o Al-Qaeda, debido a la "hibridés" de las amenazas. En conclusión, es la combinación entre lo político, lo criminal y el terrorismo hace que ciertas organizaciones sean difíciles de combatir y de desenmarañar su accionar militar, criminal o político con la finalidad de neutralizarlas.

Finalmente, a primera vista, al no percibirse de igual manera un ataque terrorista convencional (asesinato selectivo o una explosión) o una guerra, el impacto de los ciberataques o ciberguerras suele generar un gran escepticismo, sentenciando su análisis a marcas que solo se perciben en las obras de ciencia ficción. Se puede decir que los ciberataques pueden causar dificultades extremas, pero la amenaza puede ser exagerada por parte de los expertos. El impacto de las ciberguerras se encuentra inmaduro y poco desarrollado, ya que no ha ocurrido un evento político y económico de la magnitud del atentado terrorista del 11 de septiembre de 2001. El problema -y sobre esto se han elaborado especulaciones tanto en mundo académico como en la ciencia ficción- es que si toda está conectado digitalmente, ¿cual es la posibilidad que un número de hackers de otro Estado, o de una organización terrorista o una organización activista, tenga la capacidad de desactivar los equipos digitales de las Fuerzas Militares y otras agencias del Estado o, peor aún, accionar armas de destrucción masiva o sabotear infraestructura crítica?

Hay que resaltar que el fenómeno de la guerra cada vez es más denso y difícil de identificar. Esta situación hace que los objetivos, los procedimientos e incluso la identidad de las amenazas adquieran una identidad "híbrida": es el contexto en el cual los combatientes combinan sus estrategias y formas de operar con el objetivo de fortalecerse.

"HAY QUE RESALTAR QUE EL FENÓMENO DE LA GUERRA CADA VEZ ES MÁS DENSO Y DIFÍCIL DE IDENTIFICAR. ESTA SITUACIÓN HACE QUE LOS OBJETIVOS, LOS PROCEDIMIENTOS E INCLUSO **LA IDENTIDAD DE LAS AMENAZAS** ADQUIERAN UNA IDENTIDAD **"HIBRIDA":** ES EL CONTEXTO EN EL CUAL LOS COMBATIENTES COMBINAN **SUS ESTRATEGIAS Y FORMAS DE OPERAR CON EL OBJETIVO DE FORTALECERSE."**

BIBLIOGRAFÍA

Abdelgawad, A., Farstad, T. E., & Gonzalez, J. (2019, January). Vulnerability Analysis of Interdependent Critical Infrastructures upon a Cyber-attack. In *Proceedings of the 52nd Hawaii International Conference on System Sciences*.

Armitage, John, ed. *Paul Virilio: From modernism to hypermodernism and beyond*. Sage Publications. London, UK. 2000.

Caplan, Nathalie. (2013) "Cyber War: the Challenge to National Security." *Global Security Studies* 4.1

Cimadevilla, J. (2019) "De Viejas cicatrices a nuevas heridas". *Editorial Planeta*. Bogotá, Colombia.

Denning, Dorothy E. (2000) 'Cyber-Terrorism – Testimony before the Special Oversight Panel on Terrorism. Committee on Armed Services U.S. House of Representatives'. May 23 2000. The Terrorism Research Center. Extraído de: Committee on Armed Services U.S. House of Representatives (https://www.stealth-iss.com/documents/pdf/CYBERTERRORISM.pdf).

Gordon, S., & Ford, R. (2002). Cyberterrorism?. *Computers & Security*, *21*(7), 636-647.

Gray, C. (1997) "Postmodern War: The New Politics of Conflict". *The Guilford Press*.

IDC. (2019) 'IDC Forecasts Worldwide Spending on the Internet of Things to Reach $745 Billion in 2019, Led by the Manufacturing, Consumer, Transportation, and Utilities Sectors'. Framingham, *Massachusetts, US. Extraído de* (https://www.idc.com/getdoc.jsp?containerId=prUS44596319)

Knake, R. K. (2010). "Internet governance in an age of cyber insecurity". *Council on Foreign Relations.* (No. 56).

Pastor Gómez, María Luisa (2017) "Drogas, delincuencia organizada y su financiación" UNODC. Boletín IEEE, vol. 8, 2017, pp. 8-15.

Price, M. (2012). Iran and the Soft war. *International Journal of Communication*, *6*, 19.

Rid, Thomas. *Cyber War Will Not Take Place*. New York: Oxford University Press. 2013.

Tenenbaum, A. (2003) "Redes de computadoras. Cuarta Edición". *Pearson Educación de Mexico,S.A*.

Wang, H., & Wang, S. (2004). Cyber warfare: steganography vs. steganalysis. *Communications of the ACM*, *47*(10), 76-82.

EL EJÉRCITO NACIONAL FRENTE A UNA EVENTUAL GUERRA HIBRIDA EN COLOMBIA

Felipe Barrera

Politólogo de la Universidad del Rosario, Magíster en Seguridad y Defensa Nacionales de la Escuela Superior de Guerra "General Rafael Reyes Prieto" –ESDEGUE-. Coordinador de investigación de la Maestría en Seguridad y Defensa Nacionales y de la Especialización en Seguridad y Defensa del Curso de Estado Mayor -CEM-. Docente de la Escuela de Misiones Internacionales -ESMAI-.

RESUMEN

Hoy día el mundo se está enfrentando a una serie de cambios que están alterando de forma dramática la manera en la que hemos estado acostumbrados a concebir el mundo. Gracias a la tecnología, y otros hitos de la actualidad, los seres humanos hemos tenido grandes avances: el mundo se ha revolucionado y la información está al alcance de la mano, a un click de distancia.

Estos enormes cambios, sin embargo, también han tenido un impacto negativo en la seguridad de los estados, abriendo un sin fin de posibilidades a terroristas, criminales y delincuentes respecto a los medios disponibles para lograr sus fines particulares, mediante una combinación exitosa entre técnicas de guerra regular con técnicas irregulares. En este sentido, teniendo en cuenta la transformación del conflicto en Colombia, vale la pena indagar si es posible hablar de una guerra híbrida en el país -teniendo en cuenta variables concretas que van desde lo militar a lo normativo, pasando por sectores como el social, la infraestructura crítica, los medios de comunicación y la política-, con el fin de brindar una mirada prospectiva del rol del Ejército en el panorama actual de la seguridad nacional.

Palabras clave: *Guerra híbrida, terrorismo, guerra irregular, tecnología, conflicto, Colombia.*

ABSTRACT

The world is currently facing a series of changes that are dramatically altering the way we have been accustomed to conceive the world. Thanks to technology, and other milestones, human beings have made great advances, the world has been revolutionized and information is at hand, just a click away.

These enormous changes, however, have also had a negative impact on the security of states, opening endless possibilities to terrorists and criminals in terms of the means available to achieve their particular ends, through a successful combination of regular war techniques with those irregular. In this sense, taking into account Colombia's conflict transformation, it is worth investigating if it is possible to speak of a hybrid war in the country -having in mind specific variables ranging from the military to the normative, passing through sectors such as the social, critical infrastructure, the media and politics-, in order to provide a prospective view of the role of the Army in the current panorama of national security.

Keywords: *Hybrid war, terrorism, irregular war, technology, conflict, Colombia*

INTRODUCCIÓN

A lo largo de su historia republicana, el Ejército Nacional de Colombia se ha caracterizado por ser una institución íntegra, conformada por hombres valientes que han estado dispuestos a ofrendar su vida por un ideal de libertad, por los colombianos y por las instituciones de nuestro país. Ha sido una Institución compuesta por héroes de carne y hueso que, sin importar el enemigo que tengan en frente, han salido con ferocidad y con contundencia a defender la integridad de nuestro Estado.

Sin embargo, el panorama de seguridad hoy día no es el mismo al que como país hemos estado acostumbrados a vivir; es decir, un escenario donde teníamos diversos enemigos armados, con control territorial parcial en determinadas zonas del país, cuyo objetivo radicaba en llevar a cabo acciones terroristas para legitimar una supuesta lucha ideológica justificada bajo la premisa de la toma del poder político.

Hoy, además de que aún perviven los grupos descritos anteriormente, existen una serie de amenazas en la que al menos uno de los enemigos presentes en el teatro de operaciones recurre a distintas tácticas de guerra convencional y guerra irregular que simultáneamente son combinadas con acciones terroristas a través de conexiones con el crimen organizado, penetrando además las estructuras sociales. (Calvo, 2009)

Este fenómeno fue acuñado por el General James Mattis y el Teniente Coronel Frank Hoffman como guerra híbrida. Mattis y Hoffman, a través de la formulación de este concepto, lograron identificar consecuencias estratégicas y de innovación militar a la hora de enfrentarse a actores armados no estatales con ciertas capacidades que podían llegar a poner en riesgo la integridad de los Estados (Villarejo, 2014), como sucede en el caso colombiano.

Dentro de ese escenario colombiano, el Ejército Nacional, en términos de William Lind, se ha movido bajo la lógica de las guerras de cuarta generación o guerras asimétricas en la cual cambió el esquema tradicional de los conflictos, al restarle importancia a la fuerza, como recurso de poder, mientras acciones tácticas y no bélicas cobraban importancia por parte de grupos armados

“El Ejército Nacional, en términos de William Lind, se ha movido bajo la lógica de las guerras de cuarta generación o guerras asimétricas en la cual cambió el esquema tradicional de los conflictos, al restarle importancia a la fuerza, como recurso de poder, mientras acciones tácticas y no bélicas cobraban importancia por parte de grupos armados organizados.”

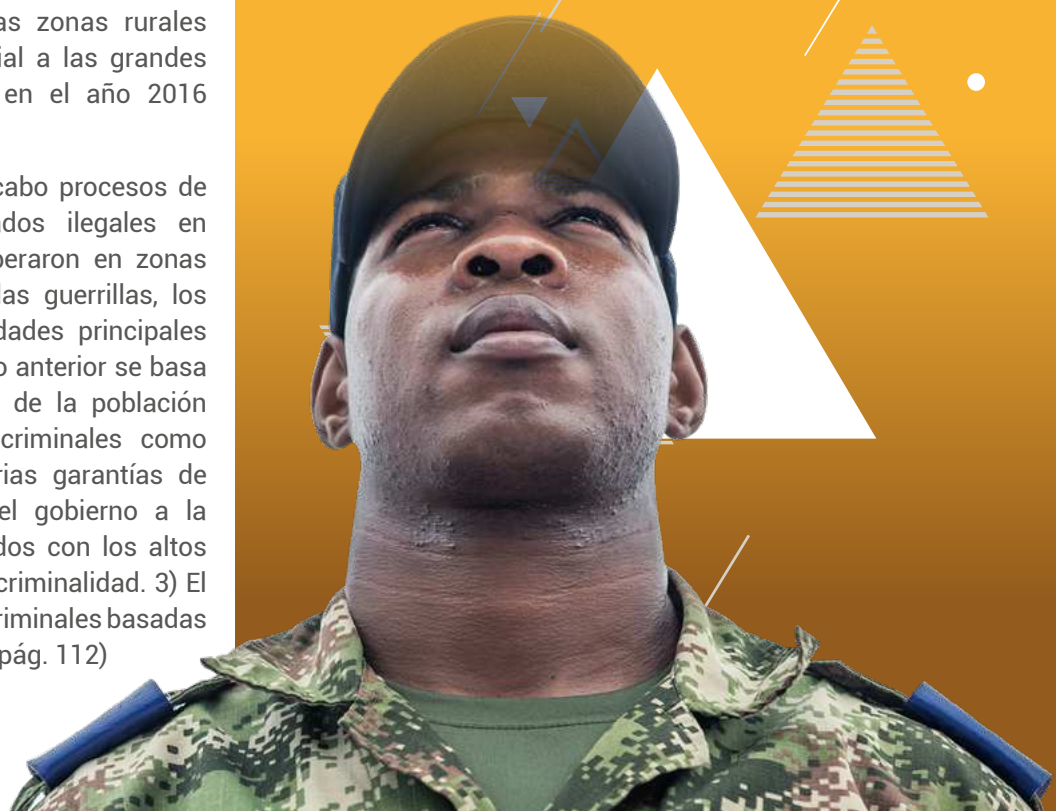
organizados (Ardila & Pinedo, 2014), que usualmente llevan a cabo acciones irregulares, teniendo en cuenta la disparidad de capacidades entre sus estructuras y un ejército regular. Tal es el caso del Ejército Nacional de Colombia.

Hoy por hoy, gracias a fenómenos como la globalización desviada, basada en las redes económicas transfronterizas que producen, se mueven y se consumen bienes tan diversos como narcóticos y animales exóticos, antigüedades y productos falsificados, dinero sucio y desechos tóxicos, así como seres humanos indocumentados en busca de trabajo. Desde la perspectiva de los autores, esta diversificación de medios ha contribuido a la consolidación del concepto de guerra híbrida, que en Colombia se ha venido manifestado de diferentes formas y escenarios y a través de diferentes actores.

A partir de la implementación de los acuerdos de paz de Santa Fe de Ralito en el año 2003 con las Autodefensas Unidas de Colombia (AUC), con la Ley 975 de 2005 o de Justicia y Paz, y posteriormente con la implementación del Acuerdo Final para la terminación del Conflicto y la Construcción de una Paz Estable y Duradera con el extinto grupo narcoterrorista, Fuerzas Armadas Revolucionarias de Colombia – Ejército del Pueblo (FARC-EP), en Colombia se ha venido presentando un fenómeno que podría ser denominado como la urbanización del conflicto, que no es más que la transición de las dinámicas de confrontación en las zonas rurales del país a las ciudades, en especial a las grandes ciudades. En un artículo escrito en el año 2016 sostenía que:

"En la medida en que se lleven a cabo procesos de desmovilización de grupos armados ilegales en Colombia, que tradicionalmente operaron en zonas rurales como los paramilitares y las guerrillas, los niveles de inseguridad en las ciudades principales del país van a tender a aumentar. Lo anterior se basa en tres razones: 1) La inclinación de la población desmovilizada a las actividades criminales como fuente de recursos. 2) Las precarias garantías de tipo socioeconómico que ofrece el gobierno a la población desmovilizada, comparados con los altos réditos económicos producto de la criminalidad. 3) El surgimiento de nuevas actividades criminales basadas en el trabajo en red." (Barrera, 2016, pág. 112)

"EN COLOMBIA SE HA VENIDO PRESENTANDO UN FENÓMENO QUE PODRÍA SER DENOMINADO COMO LA **URBANIZACIÓN DEL CONFLICTO**, QUE NO ES MÁS QUE LA TRANSICIÓN DE **LAS DINÁMICAS DE CONFRONTACIÓN** EN LAS ZONAS RURALES DEL PAÍS A LAS CIUDADES, EN ESPECIAL A LAS GRANDES CIUDADES."



En adición a las variables mencionadas, se presenta el poder político que en la actualidad tienen los ex militantes de las FARC-EP[1], el cual, sin necesidad de recurrir a prácticas criminales como en el pasado, aún cumple con el principio de la combinación de todas las formas de lucha, buscando el debilitamiento de las estructuras tradicionalistas, con el objetivo de llegar a la toma del poder absoluto en Colombia. Así, con el paso de lo rural a lo urbano, podríamos hablar del paso de una guerra asimétrica o una guerra de posiciones a una guerra híbrida o irrestricta de acuerdo a la heterogeneidad y las diferencias que implican el paso del uno a otro escenario.

Además de las formas y los escenarios en los cuales se desarrolla, una guerra híbrida involucra también una pluralidad de actores que juegan un rol preponderante en este tipo de "confrontaciones". Estos actores pueden ser Estados per se, grupos guerrilleros o grupos terroristas, redes criminales y empresas de seguridad privada (tipo blackwater). En el campo de la guerra hibrida, estos actores pueden llevar a cabo el ejercicio de diferentes medios de presión de acuerdo a los sectores en los cuales se desempeñen. De acuerdo a ello, y con base en las características del panorama actual de seguridad en Colombia, valdría la pena preguntarse si es pertinente o no hablar de una guerra híbrida en el país.

Para identificar los sectores en los cuales se desarrollan las dinámicas propias de la guerra híbrida, estos serán clasificados teniendo en cuenta un estudio presentado por Carlos Galán en diciembre del año 2018 para el Real Instituto Elcano, considerado uno de los think-tank de estudios internacionales y estratégicos de mayor relevancia en Europa. Galán llevó a cabo la clasificación de sectores de la siguiente manera: militar, social, de infraestructura crítica, medios de comunicación, político y normativo.

En lo militar, los actores adversos involucrados en el marco de la guerra híbrida adelantan acciones de una guerra no declarada en la cual emplean tropas no uniformadas y llevan a cabo acciones encubiertas, teniendo una dinámica parecida a las acciones desarrolladas por parte de los Grupos Armados no Organizados, en el marco del conflicto colombiano. Incluso, salvo por la utilización de los uniformes, podría equipararse también al actuar de las guerrillas.

A nivel social, pueden utilizar movimientos de protesta organizados por intereses partidistas o cuestiones de opinión respaldados por campañas de desinformación.

En el campo de las infraestructuras críticas[2], estas pueden llevar a cabo la negación de un servicio a través de atentados a las centrales o vías por donde los servicios son distribuidos a la población o transportados para su procesamiento como es el caso del crudo.

En el campo de los medios de comunicación, pueden llevar a cabo la elaboración de propaganda mediante el uso de redes sociales, originada en el exterior, o incluso localmente, lo que usualmente se conoce noticias falsas o fake news.

En la esfera de lo político, se pueden desempeñar a través de la diplomacia e inteligencia clásica, haciendo ejercicio de lo que en su momento el profesor Joseph Nye denominó como poder blando[3].

Finalmente, a nivel normativo los actores involucrados en las dinámicas de lo que hemos venido denominando Guerra Híbrida, llevan a cabo el aprovechamiento de las lagunas legales de un Estado para

[1] A partir del 2017, y como resultado del acuerdo de paz con las Fuerzas Armadas Revolucionarias de Co¬lombia (FARC-EP), se constituyó el partido político Fuerza Alternativa Revolucionaria del Común (FARC) cuyos fundadores fueron los ex mi¬litantes de la extinta guerrilla.

[2] "El Mayor Helber Alirio Berdugo Sierra citando a Partnering for Critical Infrastructure Security and Resilience afirma que "los sistemas y activos, ya sea físico o virtual, tan vitales para los Estados Unidos de que la incapacidad o destrucción de dichos sistemas y activos tendrían un impacto debilitante en la seguridad, la seguridad económica nacional, la salud pública nacional, la seguridad, o cualquier combinación de esos asuntos" (Berdugo, 2016, pág. 9)

[3] Es la habilidad de obtener lo que quieres a través de la atracción antes que a través de la coerción o de las recompensas. Surge del atractivo de la cultura de un país, de sus ideales políticos y de sus políticas. (Nye, 2010, pág. 118)

sacar provecho o ventaja a través de estrategias jurídicas que les permita poner a su favor la normatividad, beneficiando sus propios intereses (Galán, 2018, pág. 11).

De acuerdo con lo anterior, es posible evidenciar que las guerras de hoy en día en el mundo ya no se libran en las selvas o en los teatros de operaciones clásicos de las dos guerras mundiales o de los conflictos derivados de la denominada Guerra Fría. En esa medida, Colombia no escapa a esa dinámica: la guerra ya no es solo la confrontación directa con bandos opuestos de corte irregular y esta ya no se libra solamente en las zonas marginadas del país, donde no hay una presencia integral del Estado.

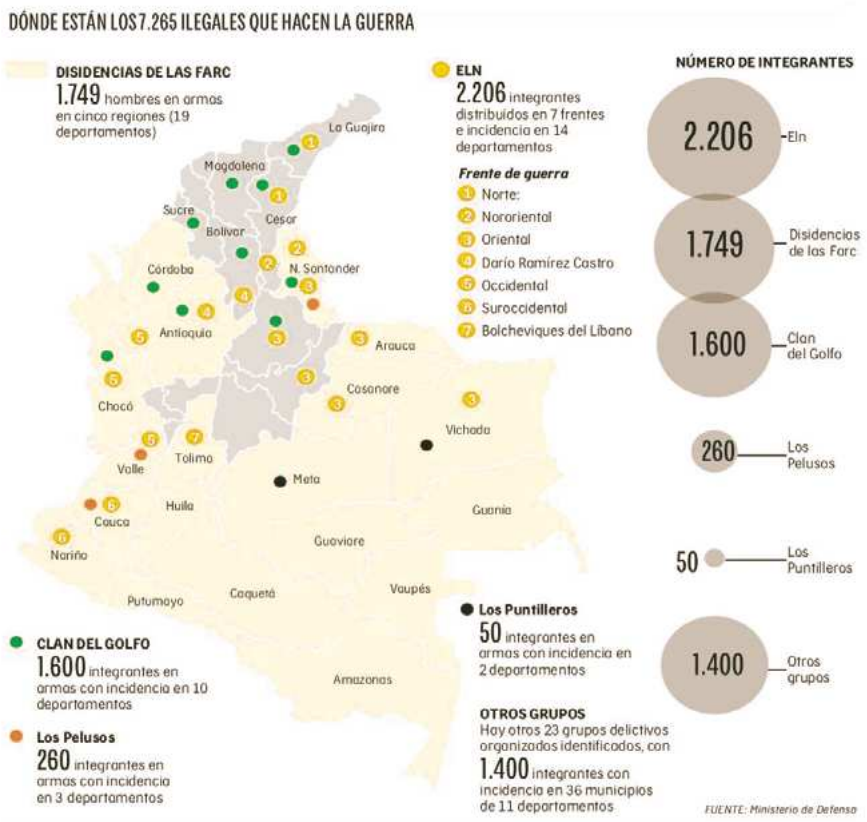
En este punto es importante resaltar que el concepto de guerra híbrida no debe recaer en una securitización de la agenda. No todo puede ser un problema de seguridad y, por ende, no todos los aspectos relativos a la seguridad deben ser responsabilidad de un único actor, como las Fuerzas Militares, en el caso particular el Ejército Nacional. Lo anterior por dos razones puntuales. Primero, porque como Estado se debe dar una respuesta integral a las problemáticas derivadas de los nuevos retos en materia de seguridad hallados bajo el marco conceptual de la guerra híbrida; segundo, porque no se debe caer en el error de calificar de enemigo a cualquier persona, partido o grupo significativo de ciudadanos que piensan de manera diferente a "X" o "Y" gobierno, respetando la institucionalidad y actuando bajo un marco normativo que establezca unas reglas de juego igualitarias para todos.

Volviendo al tema, de acuerdo con los escenarios en los cuales se manifiestan los actores en el marco de una guerra híbrida establecidos anteriormente, es pertinente hablar de una confrontación en el marco de una guerra híbrida en Colombia.

En el campo militar no es necesario hacer una búsqueda profunda para encontrar cómo los adversarios bajo la lógica de la guerra híbrida se manifiestan. Basta con citar las actividades de los Grupos Armados Organizados (GAO), como el Ejército de Liberación Nacional (ELN), las Disidencias de las FARC-EP, el Clan del Golfo, los Pelusos, los Puntilleros y otros grupos armados organizados a nivel nacional, ubicados a lo largo y ancho del territorio nacional. (Ver Imagen 1).

"A NIVEL NORMATIVO LOS ACTORES INVOLUCRADOS EN LAS DINÁMICAS DE LO QUE **HEMOS VENIDO DENOMINANDO GUERRA HÍBRIDA,** LLEVAN A CABO EL APROVECHAMIENTO DE LAS LAGUNAS LEGALES DE UN ESTADO PARA SACAR PROVECHO O VENTAJA **A TRAVÉS DE ESTRATEGIAS JURÍDICAS** QUE LES PERMITA PONER A SU FAVOR LA NORMATIVIDAD, BENEFICIANDO SUS PROPIOS INTERESES."

Fotografía:Ejército Nacional de Colombia



Fuente: (Ministerio de Defensa) Imagen N° 1 Grupos de delincuencia organizada en Colombia

Los grupos mencionados anteriormente no son una estructura criminal común, están inmersos en la variable militar en la medida en que tienen la capacidad armada para llevar a cabo enfrentamientos de alta intensidad con la fuerza pública, llegando incluso a poseer armas de largo alcance con capacidad de llevar a cabo ataques tierra-aire, como lo demostró una incautación hecha al Clan del Golfo en el año 2017 por parte del Ejército (Monsalve, 2017).

A nivel social, se ha logrado identificar la infiltración por parte de movimientos armados ilegales a espacios de legítima protesta, realizados por grupos minoritarios que claman por mayor atención y garantías del Estado. En el año 2019, en el departamento del Cauca se vivió una situación de alta peligrosidad por las protestas efectuadas por parte de La Minga indígena. Sin embargo, estas protestas no solo tenían un tinte social; según el ex fiscal Néstor Humberto Martínez, estaban contaminadas por los intereses criminales de disidencias de las FARC-EP y células del ELN que, bajo la legitimidad de la protesta indígena, querían camuflar el interés de tener el control sobre enormes cantidades de tierra libres de control y vigilancia estatal, con el fin de llevar a cabo sus actividades criminales sin ningún obstáculo.

En cuanto a la infraestructura crítica del país, durante el año 2019, específicamente durante el primer trimestre de ese año, se llevaron a cabo 23 ataques terroristas a la red de oleoductos del país, generando no solo pérdidas millonarias para el sector de hidrocarburos, que en el año 2018 fue de un total de 157.000 millones de pesos (Sáenz, 2019), sino un daño ambiental incalculable. Daño que, a diferencia de los millones perdidos, no se puede recuperar. Así mismo también se llevan a cabo atentados a las redes eléctricas, especialmente en las zonas más alejadas del país, con el objetivo de generar presión sobre el gobierno, afectando a la población civil.

En el campo de los medios de comunicación, grupos como el ELN tienen un control sobre diferentes plataformas. A diferencia de grupos como los Pelusos, los Puntilleros, etc., el ELN hoy día cuenta con plataformas radiales como Radio Nacional Patria Libre (RANPAL), Antorcha Estéreo, Radio Frontera Rebelde y Radio Insurrección Caribeña; así mismo cuenta con su propia página web llamada ELN-Paz (www.eln-paz.org) y su propia revista digital titulada Insurrección. Este tipo de plataformas se perfilan como fuentes de desinformación, de noticias falsas que generan grandes resquebrajos en la institucionalidad del Estado colombiano en la medida en que, como es evidente, se emiten o se divulgan en zonas donde, como se mencionó anteriormente, no hay una presencia integral del Estado y por ende el nivel de influencia de este tipo de medios de comunicación puede ser mayor.

Para citar un caso concreto, el Comando Central del ELN publicó un artículo en la Revista Insurrección que afirma que:

"Con este nuevo premio a militares violadores de derechos humanos se puede comprobar que se trata de una política oficial para perpetrar este exterminio, y demuestra que el terror de Estado permite a la élite dominante mantenerse en el poder. El régimen ha convertido en Doctrina Militar obligar a sus tropas a entregar cada vez más cadáveres, para demostrar buenos resultados en la lucha contrainsurgente". (Comando Central del Ejército de Liberación Nacional, 2019)

Aprovechando la coyuntura en torno a un tema cuya difusión manipulada y malintencionada tuvo un eco en la opinión pública del país, arremetiendo de manera infame contra la imagen de una institución integrada en su mayoría por seres humanos honoríficos que por convicción y amor a Colombia están dispuestos y dispuestas a ofrendar su vida, si es necesario.

En la arena política, de acuerdo a las variables de análisis planteadas por Galán, los grupos subversivos como el ELN y las FARC-EP (antes del acuerdo de paz) siempre buscaron una representatividad. Sin embargo, con el auge de las tecnologías, esta representatividad no debía, necesariamente, reflejarse a través de un partido político; es por lo anterior que el apoyo a sus "causas" se popularizó en otros países del mundo, donde la realidad del país era desconocida y ese vacío de información fue una ventana de oportunidad para lograr un apoyo internacional fuerte, que no solo se quedaba en una declaración manifiesta de apoyo, también se convertían en fuentes de financiamiento.

Danish T-shirts 'to fund rebels'

A Danish fashion firm is to sell T-shirts inspired by rebel fighters, with proceeds to go to militant groups.

The T-shirts have as logos the initials of the Revolutionary Armed Forces of Colombia (Farc) or the Popular Front for the Liberation of Palestine (PFLP).

The firm, Fighters and Lovers, says it will donate 5 euros (£3) for each T-shirt it sells.

Colombia's government has objected to the sale of the T-shirts

The Colombian government has protested to the Danish authorities over the sale of the T-shirts.

"Financing terrorist groups is unacceptable and goes against all the international norms," Colombian Foreign Minister Carolina Barco told private Caracol Radio on Friday.

"Yesterday our ambassador contacted the Danish government, we sent a protest note and have demanded an explanation."

The designers say Palestianian militant Leila Khaled and Colombian rebel leader Jacobo Arenas were among their inspirations.

Money from the sale of the T-shirts will help finance Farc radio stations in Colombia and a graphics studio in the Palestinian territories.

Fuente: (BBC News, 2006)

Imagen N° 2 Financiamiento Internacional a Grupos Ilegales colombianos

En la actualidad, la realidad a nivel nacional no dista mucho de lo que sucedió en el 2006 con este conocido caso en Dinamarca. Producto del acuerdo de paz, las FARC-EP tienen una representatividad política legal con el partido político FARC, lo cual no es malo en lo absoluto; al contrario, resulta de gran beneficio para el país que la lucha de ideas se dé en un marco de legalidad y democracia. Sin embargo, de acuerdo a la doctrina de la combinación de todas las formas de lucha no deja de ser otra vía para la toma del poder en el país. Por su parte, el ELN, que en la actualidad sigue siendo un grupo terrorista que cuenta con la permisividad y el patrocinio del gobierno de la República de Venezuela, como se evidencia en informes de inteligencia revelados por algunos medios de comunicación que rezan:

"Recuérdole lineamientos establecidos por comandante en jefe y presidente (...) que la Fuerza Armada Nacional Bolivariana en todas sus unidades y personal militar debe mantener con el Ejército de Liberación Nacional de Colombia (ELN), así como con otros grupos revolucionarios aliados a la revolución bolivariana que hacen presencia en territorio venezolano amparado en los respectivos acuerdos, que el gobierno bolivariano mantiene con dichas fuerzas revolucionarias" (El Tiempo, 2019)

A nivel normativo, existe una gran discusión por parte de diferentes partidos políticos respecto a lo que significa la Justicia Especial para la Paz (JEP). Mientras que para un sector es una ventana a la impunidad, para otros sectores es una herramienta para cumplir con los principios de verdad, justicia, reparación y garantías de no repetición a los cuales se comprometió el Estado y las FARC-EP con la firma del acuerdo.

Independientemente de las posturas en contraposición, un mecanismo que permita una aplicación normativa a los delitos cometidos durante el conflicto es necesario; sin embargo, los jueces y los custodios de este sistema deben garantizar que no se volverá un medio de impunidad en el cual los responsables de delitos de lesa humanidad, por ejemplo, no tengan una retribución con la sociedad y no paguen una pena acorde a los principios de la justicia transicional.

En conclusión, respondiendo a la pregunta que se planteó al inicio del presente escrito, Colombia es un país que está evolucionando en todos los aspectos y desafortunadamente la guerra es uno de ellos. Sí bien, como país dimos un paso para evitar la continuación de un conflicto armado, este no fue un paso para llegar a un estado de paz, como se adujo en algún momento. Como pudimos observar, los frentes de batalla son más y diversos, lo cual hace que la complejidad del conflicto haya aumentado.

"Sí bien, como país dimos un paso para evitar la continuación de un conflicto armado, este no fue un paso para llegar a un estado de paz, como se adujo en algún momento. Como pudimos observar, los frentes de batalla son más y diversos, lo cual hace que la complejidad del conflicto haya aumentado."

De acuerdo con lo anterior, nuestro Ejército debe continuar con un proceso de evolución continua, donde los valerosos hombres y mujeres que lo integran estén cada vez más preparados no solo en el arte de la guerra, como lo requirió el conflicto armado en su momento, sino además preparados a hacer frente a las amenazas que se han derivado del surgimiento de un conflicto con de características híbridas como lo describieron Mattis y Hoffman.

Es importante resaltar que debido a la naturaleza diversa de este tipo de confrontación, el país, y el Estado por supuesto, debe abandonar esa práctica de antaño en la cual toda afectación a la seguridad es responsabilidad del Ejército Nacional o sus fuerzas armadas. Como se pudo observar, las amenazas no solo están en las áreas en las que comúnmente se presentaron las confrontaciones armadas entre las Fuerzas Militares y los grupos al margen de la Ley, esta nueva dinámica de las guerras requiere de una acción conjunta, integral y coordinada por parte del Estado para poder dar respuesta a los retos que esta nueva etapa del conflicto propone.

Por otro lado, la construcción de un marco normativo que defina roles, "reglas de juego" y parámetros para el actuar de nuestros hombres y mujeres que integran la Fuerza Pública en general es necesario. Como pudimos observar en el desarrollo de este artículo, el vacío normativo es uno de los medios que pueden emplear actores adversos como una ventana de oportunidad para desarrollar libremente su accionar.

Más allá de las campañas de desinformación y los tropiezos en el camino, el Ejército Nacional de Colombia siempre ha demostrado su capacidad para defender a Colombia ante las amenazas que en el devenir de la historia hemos venido enfrentando. Aun así, la preparación para el futuro debe continuar en pro de la preservación de las instituciones y el bienestar del pueblo colombiano.

Fotografía:Ejército Nacional de Colombia

BIBLIOGRAFÍA

Villarejo, E. (Octubre de 2014). *La nueva guerra híbrida.* Obtenido de https://abcblogs.abc.es/tierra-mar-aire/otan/nuevaguerra-hibrida.html

Ardila, C., & Pinedo, C. (2014). Reflexiones sobre la Guerra de Cuarta Generación, una visión desde los actores sin recursos de poder en términos tradicionales. *Ciencia y Poder Aéreo, 9*, 79 - 87. doi:1909-7050

Gilman, N., Goldhammer, J., & Weber, S. (2013). Deviant Globalization. En I. f. Studies, *Convergence. Illicit networks and National Security in the ageo of Globalization* (págs. 3 - 14). Washington D.C: National Defense University Pres. Obtenido de https://inss.ndu.edu/Portals/68/Documents/Books/convergence.pdf

Berdugo, H. (2016). *Importancia de definir la infraestructura critica en Colombia.* Obtenido de https://repository.unimilitar.edu.co/bitstream/handle/10654/14342/BerdugoSierraHelber%20Alirio2016.pdf;jsessionid=3A2477E577EF025CB5396B6BE5BE629C?sequence=1

Nye, J. (2010). Prefacio y Capítulo 5 "El poder blando y Política Exterior colombiana". *Relaciones Internacionales*(14), 117 - 140. Obtenido de https://repositorio.uam.es/bitstream/handle/10486/678144/RI_14_7.pdf?sequence=1

Galán, C. (2018). *Amenazas híbridas: nuevas herramientas para viejas aspiraciones.* Obtenido de http://www.realinstitutoelcano.org/wps/wcm/connect/b388b039-4814-4012-acbf-1761dc50ab04/DT20-2018-Galan-Amenazas-hibridas-nuevas-herramientas-para-viejas-aspiraciones.pdf?MOD=AJPERES&CACHEID=b388b039-4814-4012-acbf-1761dc50ab04

Monsalve, R. (2017). *Incautan arsenal, con lanzacohetes incluido a "Clan del Golfo".* Obtenido de Periodico El Colombiano: https://www.elcolombiano.com/colombia/incautan-arsenal-de-clan-del-golfo-CJ6391370

Cerón, C. (2019). *Disidencias de Farc y Eln han infiltrado la minga en Cauca: Fiscalía.* Obtenido de W Radio: https://www.wradio.com.co/noticias/actualidad/disidencias-de-farc-y-eln-han-infiltrado-la-minga-en-cauca-fiscalia/20190404/nota/3886825.aspx

Sáenz, J. (2019). *Red de oleoductos ha sufrido 23 ataques terroristas en primer trimestre de 2019.* Obtenido de Periodico El Espectador: https://www.elespectador.com/economia/red-de-oleoductos-ha-sufrido-23-ataques-terroristas-en-primer-trimestre-de-2019-articulo-851642

Méndez, A. (2019). *Las 19 bandas criminales que tienen en jaque la seguridad regional.* Obtenido de Periodico El Tiempo: https://www.eltiempo.com/justicia/conflicto-y-narcotrafico/las-bandas-criminales-que-hacen-presencia-en-las-regiones-del-pais-327840

Calvo, J. (2009). La evolución de las insurgencias y el concepto de guerra híbrida. *Ejército de tierra español*(822), 6 - 13. doi:1696-7178

Barrera, F. (2016). La transformación del conflicto en Colombia: de lo rural a lo urbano. *Ensayos sobre Defensa y Seguridad, 9*, 109 - 124. doi:1794-8320

Mariño, L. (2018). *Atentado contra infraestructura eléctrica en Tumaco deja sin energía a la población.* Obtenido de Periodico La República: https://www.larepublica.co/economia/atentado-contra-infraestructura-electrica-en-tumaco-deja-sin-energia-a-la-poblacion-2705892

Comando Central del Ejército de Liberación Nacional. (2019). Recompensan con ascensos a militares de los Falsos Positivos. *Insurrección*(690). Obtenido de https://www.ranpal.net/index.php/programas/politica/la-voz-de-la-insurreccion

BBC News. (2006). *Danish T- Shirts "to found rebels".* Obtenido de BBC News: http://news.bbc.co.uk/2/hi/europe/4632578.stm

Periodico El Tiempo. (2019). *Maduro estimula al Eln para que reclute a niños en la frontera: Duque.* Obtenido de https://www.eltiempo.com/politica/gobierno/duque-dice-que-maduro-financia-a-la-guerrilla-del-eln-359772

LA MINERÍA ILEGAL EN CHOCÓ: IMPLICACIONES MEDIOAMBIENTALES Y DE SEGURIDAD. UN ANÁLISIS DESDE EL CÓDIGO DE MINAS

Isabel Botero Suárez

Politóloga de la Pontificia Universidad Javeriana con énfasis en Gestión Pública y estudiante de la maestría en Dinámicas Rurales y Globalización de la Universidad Externado de Colombia. Con experiencia en investigación, análisis y diagnóstico del contexto de seguridad en Colombia, actores y amenazas. Adicionalmente posee experiencia y habilidades específicas como docente en educación formal y no formal.

Adriana Buzón Campo

Profesional en Relaciones Internacionales con énfasis en Ciencia Política de la Universidad del Norte y Magister en Seguridad y Defensa Nacionales de la Escuela Superior de Guerra. Con experiencia en investigación en temas como seguridad y defensa, nuevas amenazas y Reforma al Sector Seguridad.

RESUMEN

La minería ilegal en Colombia ha causado grandes implicaciones sociales y ambientales, generando efectos para la seguridad territorial. El presente artículo pretende analizar, bajo el contexto institucional del Código de minas, las afectaciones al medio ambiente en el departamento del Chocó en Colombia y los retos que derivan de éste para la Fuerza Pública y el Sector Seguridad.

Palabras clave: *minería ilegal, código de minas, implicaciones al medio ambiente.*

ABSTRACT

Illegal mining in Colombia has caused vast social and environmental implications, generating a series of effects towards territorial security. The following article aims to analyze, under the institutional context of the Mining Code, environmental impacts for the department of Chocó in Colombia and challenges that arise for the Armed Forces and the Security Sector from illegal mining.

Keywords: *illegal mining, mining code, environmental implications.*

INTRODUCCIÓN

Los grupos armados ilegales han continuado diversificando sus fuentes de financiamiento, transi¬tando de una economía ilícita, principalmente enfocada en el narcotráfico, hacia la ampliación de su portafolio delincuencial orientado a mantener el desarrollo de actividades de extracción ilícita de yacimientos mineros, extorsión, secuestro, tráfico de migrantes y trata de personas, contrabando, entre otros delitos; las ganancias obtenidas culminan ya sea en lavado de activos o en financiamiento del terrorismo (UIAF, 2014).

La minería es un método para captar recursos que representa una mayor estabilidad financiera para los actores ilegales; aunque la extracción del mineral puede darse de manera ilícita, el producto que se deriva de él es comercializable de manera legal o es fácilmente legalizable.

La extracción puede darse de dos formas de acuerdo con las condiciones geológicas de formación; se encuentran los yacimientos de filón o veta, donde la explotación es subterránea y, por otro lado, de tipo aluvión, con explotación a cielo abierto (Ministerio de Justicia de Colombia & UNDOC, 2016).

El oro, además, tiene unas particularidades que se presentan beneficiosas, como la extracción de relativamente baja complejidad especialmente del tipo aluvial, de fácil procesamiento y transportabilidad ligera, que es útil también para el lavado de activos (Contraloría General de la República, 2013).

Estas características, sumadas a la condición periférica de los lugares donde se desarrollan estas actividades de manera ilegal, han generado que los impactos sociales y ambientales de la minería sean mucho mayores; así como los beneficios para los grupos armados.

LA POLÍTICA DE MINAS EN COLOMBIA

El Código de Minas en Colombia, promulgado bajo la Ley 685 de 2001, le otorga al Estado colombiano el rol de facilitador, promotor, regulador y fiscalizador de la actividad minera. Su diseño y debates se dieron durante una época de recientes cambios económicos, pues durante la década anterior el país había impulsado un modelo neoliberal que alentaba a los inversionistas extranjeros a traer sus capitales y, según la Contraloría General de la República CGR (2013), indirectamente generaba incentivos a los nacionales para desarrollar esta actividad de manera ilegal:

La política de incentivos tributarios para la inversión, como son las exenciones de IVA a exportadores, exclusión en la renta presuntiva, excepción de la retención en la fuente, acreditación de exportaciones mineras como productos verdes, sistema de amortización, Plan Vallejo, subsidio a combustibles en zonas de frontera que operaron hasta el 2011, como instrumentos que benefician a grandes empresas exportadoras. Es evidente la mella que se genera en la conciencia tributaria ciudadana, que conlleva evidentemente a facilitar la consideración de la alternativa ilegal. (pág. 4)

Al mismo tiempo, el ente de control advierte que la falta de armonización entre las políticas mineras y de vías y transportes han dejado en el abandono a regiones enteras que subsisten a partir de esta actividad, reforzando las tendencias hacia la ilegalidad (CGR, 2013). Algunos de los medios institucionales para formalizar a los pequeños mineros se fueron convirtiendo con el tiempo en incentivos perversos que alimentaban la ilegalidad del sector, en la medida en que fueron incrementando el tiempo necesario para la legalización de la actividad.

El Decreto 2636 de 1994 exigía existencia como minero sin titulo con fecha anterior al 30 de septiembre de 1993, el Decreto 2390 de 2002, existencia anterior al 17 de agosto de 2001 y si se revisa el proceso de legalización que generó la Ley 1382 de 2010, puede observarse que la exigencia de requisitos del Decreto 2715 de 28 de julio de 2010 es mucho más alta, por cuanto se requiere la demostración de 10 años de antigüedad y 5 años de continuidad en la extracción minera. (Contraloría General de la República, 2013)

Fotografía:Ejército Nacional de Colombia

" LA FALTA DE ARMONIZACIÓN **ENTRE LAS POLÍTICAS** MINERAS Y DE VÍAS Y TRANSPORTES HAN DEJADO EN EL ABANDONO A **REGIONES ENTERAS** QUE SUBSISTEN A PARTIR DE ESTA ACTIVIDAD."

"LAS POLÍTICAS DE SEGURIDAD **ALREDEDOR DE LA MINERÍA**, POR SU PARTE, **NO HAN DIFERENCIADO** DE MANERA CLARA LAS DISTINCIONES ENTRE **LA MINERÍA INFORMAL-ILEGAL MECANIZADA Y LA MINERÍA CRIMINA ;** POR LO QUE LA FUERZA PÚBLICA NO CUENTA CON LINEAMIENTOS QUE LE PERMITAN EJERCER UN TRATAMIENTO DIFERENCIAL **FRENTE A ESTOS TEMAS."**

Fotografía:Ejército Nacional de Colombia

A pesar de lo anterior, el Código de Minas avanzó en el reconocimiento de proyectos mineros especiales, donde se abre la posibilidad de hacer desarrollos comunitarios y el establecimiento de unos criterios de minería tradicional; aunque no presenta iniciativas para hacerla competitiva en el mercado global, atándolo a técnicas de extracción que no permiten la utilización de maquinaria especializada y, en este sentido, impidiendo la modernización de la actividad para las comunidades que históricamente han desarrollado la minería de oro.

Las políticas de seguridad alrededor de la minería, por su parte, no han diferenciado de manera clara las distinciones entre la minería informal-ilegal mecanizada y la minería criminal; por lo que la Fuerza Pública no cuenta con lineamientos que le permitan ejercer un tratamiento diferencial frente a estos temas.

LA MINERÍA ILEGAL EN EL DEPARTAMENTO DEL CHOCÓ

Para el año 2011 el 18% de la producción de oro en Colombia provenía de explotaciones de yacimientos de veta y el 82% correspondía a las explotaciones de aluvión. En 17 de los 32 departamentos del país hay evidencia de explotación de oro de este último tipo, de los cuales el 24% se encontraba en los departamentos del litoral Pacífico y el 46% en el departamento del Chocó, principalmente a las orillas del rio San Juan. (Contraloría General de la República, 2013). El Centro de Estudios para la Justicia Social escribió en el año 2016 el informe La minería en el Chocó en clave de derechos: Investigación y propuestas para convertir la crisis socio ambiental en paz y justicia territorial donde, basados en los variables de Kambani (2003; citado en CEJS, 2016), establecen algunas características que permiten que el fenómeno de la minería ilegal en el Chocó se haya mantenido en el tiempo.

La primera de ellas es la falta de acceso a derechos mineros, donde además de los obstáculos legales mencionados anteriormente , hacen explícito que los procesos que se han venido dando entre 1998 y 2010 no han sido exitosos en cuanto al número de minas legalizadas. Sin embargo, el inicio de dichos procesos ha permitido que las minas que se encuentran a la

La inversion para el fortalecimiento institucional tampoco ha sido un factor que facilite la legalización de la minería en este departamento.

espera de ser legalizadas sean protegidas de acciones penales en su contra, hasta que la autoridad minera se pronuncie al respecto. Así mismo, señala las demoras y procesos burocráticos por las que deben pasar las comunidades. afrodescendientes o indígenas para legalizar y reglamentar una zona minera (CEJS, 2016).

La segunda hace referencia a unos marcos institucionales de apoyo débiles. Se refiere a situaciones donde las instituciones que tienen responsabilidades alrededor de los temas ambientales y mineros no cuentan con la dotación necesaria para llevar a cabo sus tareas. Esto, bajo la premisa de que en la medida en que el marco institucional sea fuerte, la minería tiende a la legalización (CEJS, 2016).

Los recursos asignados al sector ambiente y sector minero para el departamento de Chocó son mínimos. Por un lado, la ejecución presupuestal de los proyectos de inversión en Chocó para el sector de Minas ha oscilado alrededor de los seis mil millones de pesos en los últimos años, mientras que el sector de ambiente y desarrollo sostenible no alcanza una sexta parte de ese monto. Por otro lado, aunque ninguno de los sectores analizados en el Chocó alcanza a representar el 1% del Presupuesto General de la Nación, el porcentaje en el sector de minas fue en promedio diez veces mayor al de ambiente en los últimos tres años. Sin poder pronunciarnos sobre las causas o efectos netos de estas asimetrías presupuestales, estas brechas sugieren que las prioridades estatales no se encuentran en el Chocó y que, los recursos que se disponibilizan,

Fotografía:Ejército Nacional de Colombia

en realidad le apuestan a la minería y su fomento y dejan en último plano la preservación y planificación ambiental (CEJS, 2016).

Por lo tanto, la inversion para el fortalecimiento institucional tampoco ha sido un factor que facilite la legalización de la minería en este departamento.

La tercera, por último, hace referencia a las condiciones de seguridad y problemas de orden público, donde aseguran que a pesar de las conflictividades sociales y la presencia de diferentes actores armados en el departamento, no todos los Consejos Comunitarios Mayores donde se desarolla la minería ilegal presentan condiciones críticas de seguridad (CEJS, 2016).

En términos económicos Colombia produjo y exportó en el año 2015 1'903.386 onzas de oro, pero sólo 220.000 fueron extraídas de minas con títulos mineros legales (Vargas, 2016); lo que significa que menos del 12% de ese mineral fue extraído bajo unos estándares ambientales que procuran por la sostenibilidad productiva y ambiental.

El estudio realizado por la Contraloría (2013) revela que las formas de extracción ilegal del oro aluvial en el departamento del Chocó con uso de maquinaria de tierra tiene cinco etapas: 1) preparación del terreno con vías de acceso para personal y transporte del material y adecuación del suelo sin vegetación en los alrededores donde se presumen los yacimientos, entre otros; 2) se dan las actividades de excavación de las arenas y gravas, luego acopiarlas en el mismo lugar y el beneficio se realiza con técnicas que pueden ser físicas, mecánicas o artesanales clasificación y separación por tamaños o gravedad, así como a través de técnicas químicas como la amalgamación con mercurio o cianuro; 3) con el reconocimiento del suelo, la forma de extracción y tecnificación de las tareas, se empieza a obtener un producto más puro; 4) al mismo tiempo, surgen subproductos que también pueden ser aprovechados como la plata y el platino; 5) las medidas restaurativas con el medio ambiente contempladas en el código de minas no son puestas en acción por este tipo de minería, una vez la mina ha sido extraída, la mina es abandonada y se buscan áreas cercanas para iniciar de nuevo todo el proceso de explotación.

De este trabajo, el personal de la mina recibe menos de $15.000 por un gramo de oro que en promedio alcanza a extraer diariamente, y de los cuales debe invertir casi el 25% en la gasolina para la motobomba utilizado en el procesamiento químico. Esta situación da cuenta de las necesidades básicas insatisfechas del departamento, pues la falta de oportunidades impulsa a los pobladores a mantenerse en esta actividad, a pesar de que la retribución no es tan alta (Naverrete & Latam, 2017).

" LAS MEDIDAS RESTAURATIVAS CON EL MEDIO AMBIENTE CONTEMPLADAS EN EL **CÓDIGO DE MINAS** NO SON PUESTAS EN ACCIÓN POR ESTE TIPO DE MINERÍA, **UNA VEZ LA MINA HA SIDO EXTRAÍDA, LA MINA ES ABANDONADA** Y SE BUSCAN ÁREAS CERCANAS PARA INICIAR DE **NUEVO** TODO EL **PROCESO DE EXPLOTACIÓN**."

Fotografía:Ejército Nacional de Colombia

IMPLICACIONES MEDIOAMBIENTALES DE LA MINERÍA ILEGAL EN EL CHOCÓ

Además de las condiciones de inseguridad social que deriva del actuar de grupos ilegales en el marco de la extracción ilícita de yacimientos mineros en el departamento del Chocó y de las condiciones institucionales que facilitan dicha actuación, el problema abordado merece considerar las implicaciones al medio ambiente generadas por esta práctica, pues "casi la mitad de la cubierta forestal se ha perdido en el país a causa de las actividades mineras en Chocó" (Semana Sostenible, 2018), y este departamento se ubica en el peor nivel de contaminación de fuentes hídricas debido al empleo del mercurio en las prácticas extractivas.

La Defensoría del Pueblo, en su informe de 2015 titulado La minería sin control, presentó sus consideraciones frente a los principales problemas asociados a la minería, para lo cual, en aspectos medio ambientales, reconoció que el impacto negativo se da en tres espectros: agua, suelo y aire.

En cuanto a la contaminación de las fuentes hídricas, el río Atrato es de los principales afectados; en la margen izquierda del cauce de este río, "el material removido —conglomerado— es arrastrado por la corriente de agua, produciendo sedimiento" (Defensoría del Pueblo, 2015), y paralelo a ello, la contaminación se ha exacerbado en los últimos años a razón de la disposición de químicos que se emplean en esta actividad. Por otro lado, el río Quito, intervenido por los actores involucrados en la extracción —sobre todo a la altura de los corregimientos de San Isidro, Villa Conto y La Soledad—, ha sufrido de cambios en su cauce principalmente por la tala del bosque tropical húmedo a su orilla; esto ha generado el aumento de la playa y la saturación de la misma por el exceso de sedimiento.

En este sentido, la Defensoría del Pueblo (2015) concluye que "la sobreexplotación de los minerales en el cauce de los ríos ha hecho que el perímetro mojado, el radio hidráulico y por consiguiente su perfil cambien de forma considerable"(pág. 67). Además, reconoce las implicaciones para la salud de los pobladores y la pesca que se da en las zonas más afectadas debido a la contaminación excesiva del agua a razón de los minerales que se emplean en los procesos extractivos.

En cuanto a las implicaciones referentes al suelo y la vegetación en las zonas de extracción, las principales afectaciones se evidencian en la tala del bosque tropical húmedo, con el fin de expandir la frontera minera, lo que ha generado impactos negativos para el material vegetal nativo del departamento.

Fotografía:Ejército Nacional de Colombia

"LOS PROBLEMAS ASOCIADOS A LA **EXTRACCIÓN ILÍCITA DE YACIMIENTOS MINEROS** RESPECTO AL MEDIO AMBIENTE SON MÚLTIPLES, Y PARTICULARMENTE PARA EL **DEPARTAMENTO DEL CHOCÓ,** LAS PROYECCIONES A FUTURO SOBRE SU **SOSTENIBILIDAD AMBIENTAL SON CRÍTICAS."**

La deforestación, entonces, se constituye como la principal afectación al suelo derivada de la extracción ilícita de yacimientos mineros. En este contexto, el IDEAM (2018) reporta que para 2017 la deforestación en el departamento del Chocó constituía el 4,6% del porcentaje total nacional, con 10.046 hectáreas que ubicaron a este departamento en el sexto lugar, solo después de Caquetá, Guaviare, Meta, Antioquia y Putumayo.

Finalmente, la contaminación del aire constituye la última implicación medio ambiental que genera la minería ilegal en este departamento, principalmente debido a las emisiones atmosféricas del proceso extractivo de oro y plata.

La minería produce emisiones a la atmósfera, tanto sólidas, polvo en las voladuras, carga y transporte, como gases que pueden ser: I) gases de combustión de la maquinaria del proceso minero (combustión de hidrocarburos, gasolina y diésel); II) gases liberados durante el proceso de extracción (CO2 y CO y el grisú, mezcla altamente explosiva de metano y aire); III) gases provenientes de las voladuras y IV) gases de los procesos de la actividad minera (COx , NOx , SOx y SO2). También se emiten aerosoles que usualmente están cargados en compuestos que puedan tener riesgo ambiental y que son emitidos durante la explotación en los procesos de hidrometalurgia (sulfúrico para la extracción de cobre y cianuro para la extracción del oro). (Defensoría del Pueblo, 2015, pág. 179).

En resumen, los problemas asociados a la extracción ilícita de yacimientos mineros respecto al medio ambiente son múltiples, y particularmente para el departamento del Chocó, las proyecciones a futuro sobre su sostenibilidad ambiental son críticas.

Fotografía:Ejército Nacional de Colombia

CHOCÓ: UNA MINA DE ORO PARA LOS GRUPOS ILEGALES

Las características sociales, institucionales, geográficas y geológicas del departamento del Chocó han consolidado algunas condiciones que se presentan como una ventana de oportunidad para los actores ilegales.

En primer lugar, el tipo de oro allí presente, aluvial, de fácil extracción y procesamiento, ha configurado alrededor de él cadenas de producción ilegales-informales que representan un beneficio económico; aún cuando tienen el riesgo de ser procesados penalmente.

En segundo lugar, los obstáculos que se presentan normativa y administrativamente para legalizar los títulos mineros, tanto de las comunidades como de los privados, constituyen la promoción del sostenimiento de la ilegalidad.

Por otro lado, la debilidad institucional en la región y a nivel local representada a través de entes gubernamentales y de control, infraestructura, servicios públicos, etc., tampoco favorece el tránsito a la legalidad.

Finalmente, la característica de fácil legalización de un producto obtenido de manera ilícita, hace del oro uno de gran valor, especialmente en aquellos territorios donde la ilegalidad ha permeado distintos eslabones sociales y económicos.

Los actores ilegales han aprovechado este territorio para obtener ganancias y diversificar su portafolio. Son éstos los que cobran 'impuestos' por la extracción y comercialización de oro; pero estos grupos no se han dedicado solamente al control. Por las características aquí expuestas, también han entrado en el negocio adquiriendo maquinaria propia y pagando trabajadores (Semana Sostenible, 2019).

Investigaciones recientes señalan estrategias como la inscripción de personas muertas o inexistentes como barequeras en los registros únicos del Ministerio de Minas.

El material probatorio del ente investigador, reveló transacciones elevadas con proveedores sin capacidad económica (barequeros) para respaldar millonarios negocios que representaron la suma de US$218.000.000. Este tipo de suplantaciones tienen dos propósitos esenciales: el primero es simular envíos de oro "fantasma" que permitan legalizar grandes movimientos de dinero en el extranjero, y por otro lado están aquellas exportaciones de oro ilegal camuflado que pueda ser distribuido en los mercados de Estados Unidos y Europa de forma legal. (InSight Crime, 2019)

La no distinción legal, entonces, entre los mineros ilegales-informales y la minería desempeñada por gupos ilegales sólo representa una ventaja más para estos últimos.

> *"Los actores ilegales han aprovechado este territorio para obtener ganancias y diversificar su portafolio. Son éstos los que cobran 'impuestos' por la extracción y comercialización de oro; pero estos grupos no se han dedicado solamente al control."*

En el país, y en particular en el departamento del Chocó, debería ser discutido si el modelo planteado por el Código de Minas responde a las necesidades territoriales. La formalización implica que el Estado tiene un control sobre los procesos, lo que facilita el monitoreo de cuestiones ambientales, tributarias, comerciales, entre otros.

La debilidad del Estado no genera encadenamientos productivos que permitan diversificar oportunidades productivas en el territorio, por el contrario, se diversifica el portafolio de los actores ilegales.

Estas dinámicas han generado un incremento en las afectaciones al medio ambiente en el departamento de Chocó, particularmente en cuanto a deforestación y contaminación de fuentes hídricas y la ausencia de medidas restaurativas para el medio ambiente impuestas por el Código de Minas; cuyas proyecciones a futuro determinan la ausencia de sostenibilidad, no solo para los pobladores, sino también para los ecosistemas de la región. La respuesta del Estado en contra de la minería ilegal, por tanto, debe ser unificada. Su actuación debe recoger iniciativas factuales no solo en función de las herramientas legales disponibles para la distinción de los actores involucrados en las prácticas mineras, sino también en los marcos de participación de los entes de control y la Fuerza Pública, así como de las alternativas productivas disponibles en el territorio para los pobladores que se desempeñan en funciones extractivas irregulares.

BIBLIOGRAFÍA

Rivera, A. (2014). *Minería aurífera en el Bajo Cauca antioqueño*. Obtenido de Revista Zero. Universidad Externado de Colombia: https://zero.uexternado.edu.co/mineria-aurifera-en-el-bajo-cauca-antioqueno/

Contraloría General de la República. (2013). *Informe especial Minería ilegal: La explotación ilícita de recursos minerales en Colombia. Casos valle del Cauca (río Dagua)- Chocó (Río San Juan) efectos sociales y ambientales.* Bogotá D.C.

Ministerio de Justicia de Colombia, & UNDOC. (2016). *Explotación de oro de aluvión Evidencias a partir de percepción remota.* Bogotá.

CEJS. (2016). *La minería en el Chocó en clave de derechos: Investigación y propuestas para convertir la crisis socio ambiental en paz y justicia territorial.* Bogotá: Centro de Estudios para la Justicia Social (CEJS).

Vargas, P. (10 de junio de 2016). *Así 'lavan' el oro de la minería ilegal en el país*. Obtenido de Portafolio: https://www.portafolio.co/economia/gobierno/lavan-oro-mineria-ilegal-pais-497191

Naverrete, T., & Latam, M. (23 de junio de 2017). *La lucha de un consejo comunitario contra la minería ilegal en Chocó*. Obtenido de Semana Sostenible: https://sostenibilidad.semana.com/medio-ambiente/articulo/mineria-ilegal-en-choco-la-lucha-de-un-consejo-comunitario-contra-la-mineria/38094

Semana Sostenible. (21 de marzo de 2019). *Luchan contra la minería ilegal en el Chocó*. Obtenido de Medio ambiente: https://sostenibilidad.semana.com/medio-ambiente/articulo/luchan-contra-la-mineria-ilegal-en-choco/43440

InSight Crime. (6 de mayo de 2019). *Empresarios de oro de Colombia usaron mineros falsos y muertos para lavar dinero*. Obtenido de InSight Crime: https://es.insightcrime.org/noticias/analisis/empresarios-de-oro-de-colombia-usaron-mineros-falsos-y-muertos-para-lavar-dinero/

Semana Sostenible. (6 de febrero de 2018). *Chocó, epicentro de los conflictos sociales y ambientales en Colombia*. Obtenido de Medio ambiente: https://sostenibilidad.semana.com/medio-ambiente/articulo/choco-epicentro-de-los-conflictos-sociales-y-ambientales-en-colombia/39447

Defensoría del Pueblo. (2015). La minería sin control. Bogotá: Defensoría del Pueblo.

InSight Crime. (2018). La nueva generación de narcotraficantes colombianos post-FARC: "Los Invisibles". Obtenido de https://es.insightcrime.org/wp-content/uploads/2018/03/La-nueva-generaci%C3%B3n-de-narcotraficantes-colombianos-post-FARC-Los-Invisibles.pdf

UIAF. (2014). Riesgo de lavado de activos y fi nanciación del terrorismo en el sector de transporte de carga terrestre. Obtenido de http://www.urosario.edu.co/observatorio-de-lavado-de-activos/Archivos_Lavados/Riesgo-de-LAFT-sector-transporte-carga-terrestre.pdf

IDEAM. (2017). *Resultados Monitoreo de la Deforestación 2017.*Obtenido de http://www.ideam.gov.co/documents/24277/72115631/Actualizacion_cifras2017+FINAL.pdf/40bc4bb3-370c-4639-91ee-e4c6cea97a07

LA GUERRA DEL FUTURO YA HA COMENZADO Y BRASIL ENFRENTA EL DESAFÍO DEL ABISMO TECNOLÓGICO

Peterson Ferreira da Silva

Doctor en Relaciones Internacionales (IRI-USP), profesor del campus Brasilia de la Escuela Superior de Guerra (ESG) e investigador del Centro de Estudios Estratégicos del Ejército (CEEE) entre el 2016 y el 2018. Este artículo, así como las ideas, datos e informaciones en los contenidos, expresan el pensamiento del autor, siendo de su entera responsabilidad, sin representar necesariamente la posición del Ministro de Defensa, de la Escuela Superior de Guerra o el Ejército brasileño.

RESUMEN

El objetivo de este ensayo es explorar los impactos que determinadas tecnologías avanzadas pueden traer en los próximos años para las más modernas fuerzas militares del mundo. Este trabajo revela algunas de las posibilidades de los campos de la inteligencia artificial, el Internet de las cosas y las tecnologías autónomas. A partir del breve análisis desarrollado es posible sugerir estudios más detallados buscando la identificación, la interacción y la priorización de líneas tecnológicas de intereses compartidos entre las áreas de inteligencia, defensa y seguridad pública en Brasil.

Palabras clave: *Fuerzas Armadas, Defensa, Inteligencia, Seguridad Pública, Tecnología.*

ABSTRACT

The purpose of this paper is to explore the impacts that certain advanced technologies (including their organizational spin-offs) may bring in the coming years to the most modern armed forces. This text points out some of the possibilities unveiled by the fields of artificial intelligence, additive manufacturing, the Internet of Things (IoT) and autonomous technology. From the brief analysis developed, the author suggests the development of more studies seeking to intensify, interact and prioritize technological lines between the areas of intelligence, defense and law enforcement in Brazil.

Keywords: *Armed Forces, Defense, Intelligence, Law Enforcement, Technology.*

EL PROBLEMA: LA "COMPETENCIA DE LA REINA ROJA"

Los acelerados descubrimientos tecnológicos asociados a vehículos autónomos, robótica avanzada, inteligencia artificial y el internet ya están presentes en los planes de las más modernas fuerzas militares alrededor del mundo. El desarrollo de estas tecnologías puede afectar, sobre todo, a los principales centros del poder político en toda su extensión organizacional, por medio de campañas de desinformación y de manipulación de la opinión pública, las cuales encuentran terreno fértil en el ciberespacio. Ese conjunto de nuevas tecnologías puede modificar, por ejemplo, el funcionamiento de las redes sociales, propagandas, bolsas de valores, mercados y visiones políticas alrededor del mundo.

Dado el paso acelerado de las innovaciones tecnológicas, los países pasaron a tener que avanzar cada vez más rápido, solo para continuar en la misma posición (no quedarse relegados frente a otras naciones) y no para escalar - comparación recurrentemente utilizada en la hipótesis de la Reina Roja o efecto Reina Roja contenida en la renombrada obra de Lewis Carroll.

En ese contexto, una de las cuestiones a ser tenidas en cuenta por las fuerzas armadas de países como Brasil, ya no consiste en definir cómo lidiar con los vacíos de conocimiento con relación a determinadas tecnologías, sino a cubrir los gaps (o brechas) asociados al creciente abismo tecnológico concerniente a todo un conjunto de transformaciones que son ajenas a los sectores de defensa nacional.

EL NACIMIENTO DE LA GUERRA ROBÓTICA

Cuando Peter W. Singer publicó su libro Wired for War (2009) más de doce mil equipos utilizando tecnología autónoma estaban siendo empleados en Irak, la guerra robótica se mostraba como el elemento más certero en medio de la euforia inicial de la denominada Revolución de los Asuntos Militares (RAM). Hoy, los drones son cada vez más sofisticados y armados, como, por ejemplo, el dron británico Protector que puede cargar misiles avanzados, bombas guiadas por láser y radar por más de 40 horas (Jennings, 2018). Además, los vehículos no tripulados están cada vez más presentes también en tierra y en las profundidades del océano. Los vehículos no tripulados navales de superficie se han venido configurando para desempeñar funciones antiminas, antisubmarino, de guerra electrónica y de seguridad marítima.

> *"El desarrollo de estas tecnologías puede afectar, sobre todo, a los principales centros del poder político en toda su extensión organizacional, por medio de campañas de desinformación y de manipulación de la opinión pública, las cuales encuentran terreno fértil en el ciberespacio."*

Fotografía: http://www.eb.mil.br/

La madurez de las tecnologías asociadas a los vehículos autónomos y/o tripulados de forma remota ha suscitado una serie de reflexiones en diversos sectores, las cuales han derivado en la innovación de productos, procesos y marketing, especialmente, organizacionales. Los propios entrenamientos militares empezaron a sufrir modificaciones y adaptaciones para emplear adecuadamente estos nuevos sistemas en el marco de sus doctrinas. Por ejemplo, el ejercicio multinacional británico Unmanned Warrior exigió un ambiente controlado para que los países participantes pudieran probar y evaluar sus vehículos no tripulados aéreos, navales de superficie y minisubmarinos, así como la conectividad y el trabajo en equipo entre estas diferentes tecnologías (Freedberg Jr., 2016).

CUANDO NUEVAS TECNOLOGÍAS ENCUENTRAN VIEJAS TECNOLOGÍAS

El campo de la inteligencia artificial (IA) también ha despertado interés de los militares para su aplicación en entrenamientos, simulaciones y experimentos en campo, de la mano de la realidad virtual y aumentada. Siendo objeto de inversiones millonarias en los próximos años por parte de los EE. UU., los proyectos de inteligencia artificial piensan introducirse en el campo de tecnologías autónomas, por ejemplo, mediante el empleo de "enjambres" de minidrones, que pueden saturar defensas enemigas, identificando, clasificando y priorizando blancos rápidamente (Knapp, 2018).

Paralelamente, las plataformas militares y sistemas de armas convencionales, como submarinos, fragatas y sistemas de misiles siguen siendo perfeccionados y cada vez más efectivos, a medida que han sido perfeccionados con nuevas tecnologías.

El barco de guerra más avanzado, el USS Zumwalt (DDG- 1000), no sólo exterioriza el estado del arte de las tecnologías furtivas aplicadas al medio naval sino también el uso de plataformas para misiles multimisión (tierra, antinavio y antimisiles balísticos) y de alcance extendido (Larter, 2018). Cabe resaltar que los misiles supersónicos y convencionales siguen renovándose, algunos de ellos ya se producen con ayuda de impresoras 3D (Raytheon, 2017). Cazas y submarinos ya prueban las posibilidades de trabajo

en equipos con plataformas no alquiladas; además, la existencia de indicios sobre un proyecto de un dron submarino ruso que se ha movido y armado nuclearmente ya provoca reacciones de analistas militares norteamericanos (Star, Cohen, 2018; Insinna, 2018). Los sistemas de armas de energía dirigidas (láser) (Lockheed Martin, 2018) y proyectos de cañones electromagnéticos (railgun) en los EE.UU. y en China (Brimelow, 2018), son ejemplos ilustrativos de la magnitud de la transformación en curso. Todos estos nuevos paradigmas representan, al mismo tiempo, oportunidades y vulnerabilidades, que ponen a prueba la capacidad de las organizaciones de adaptar y gestionar los cambios, con el fin de aprovechar al máximo (en los medios civil y militar) el ascenso de estas nuevas tecnologías.

DÁNDOLE SENTIDO AL OCÉANO DE INFORMACIÓN

El área de análisis del gran volumen de datos (big data) también se puede destacar en tanto sus posibles aplicaciones militares se están explorando, especialmente en lo que se refiere a la simulación, así como en las actividades de prueba y evaluación. El uso de big data ganó impulso en las últimas décadas en el ámbito civil, junto con el avance observado en las Tecnologías de Información y Comunicaciones (TIC), sobre todo con la aparición de las nubes de información y el incremento de las técnicas de fusión y minería de datos. En este sentido, la Agencia Europea de Defensa (EDA), por ejemplo, ha venido explotando de forma cooperativa la potencialidad de este campo para la defensa (EDA, 2017).

"SIENDO OBJETO DE INVERSIONES MILLONARIAS EN LOS PRÓXIMOS AÑOS POR PARTE DE LOS EE. UU., **LOS PROYECTOS DE INTELIGENCIA ARTIFICIAL** PIENSAN INTRODUCIRSE EN EL CAMPO DE **TECNOLOGÍAS AUTÓNOMAS,** POR EJEMPLO, MEDIANTE EL EMPLEO DE **"ENJAMBRES"** DE MINIDRONES, QUE PUEDEN SATURAR DEFENSAS ENEMIGAS, **IDENTIFICANDO, CLASIFICANDO Y PRIORIZANDO** BLANCOS RÁPIDAMENTE."

Fotografía: http://www.eb.mil.br/

La tecnología avanzada de los proyectos de investigación (IARPA, 2018), por medio de su programa bautizado Mercury, ha intentado utilizar los conocimientos de campo para transformar las avalanchas de datos e información públicamente disponibles, para prevenir eventos como crisis económicas e inclusive epidemias. Se suma a ello el impacto de Internet de las cosas (Internet of Things -IoT-), abriendo todo un abanico de posibilidades y de amenazas cibernéticas no sólo para las fuerzas armadas y las infraestructuras críticas sino también para las economías nacionales. Tal realidad viene demandando mayores esfuerzos de planificación interagencial e involucrando a diversos actores nacionales, incluido el sector privado:

> If national defense policy is to address the new challenges posed by the Internet of Things, then it may be necessary to broaden existing joint and interagency planning approaches into a more comprehensive 'Whole of Nation' approach (Deloitte, 2017, p. 18).

Además, este conjunto de nuevas tecnologías trae un amplio orden de cambios, más allá de los tradicionales ends, ways y means de los estrategas, generando así reflexiones sociales, políticas y culturales. Después de todo, existe una necesidad urgente por parte de la academia de introducir "una nueva reflexión sobre las implicaciones de la Cuarta Revolución Industrial para la seguridad internacional" (Kasperse, Eide, Shetler-Jones, 2016), incluida la transformación de los medios sociales en armas (Singer, Brooking, 2018).

En este marco, el concepto de resiliencia viene ganando cada vez más importancia en los debates sobre seguridad y defensa nacional, porque se trata, genéricamente, de buscar la capacidad para que el Estado se adapte constantemente a nuevas vulnerabilidades y amenazas emergentes, absorbiendo crisis y ataques y coordinando iniciativas civiles y militares en nivel estratégico (Otan, 2016).

Fotografía: http://www.eb.mil.br/

EL CASO BRASILERO

En Brasil, se observa, de forma general, que existen una serie de dificultades para acompañar estos avances tecnológicos de vanguardia de las principales potencias. Primero, es necesario subrayar que la ciencia en Brasil, a nivel general, se encuentra inmersa en problemas que, más allá de la falta de financiación, se explican a causa de la falta de visión estratégica de gobierno y de una política de Estado que comprenda la necesidad de aumentar las inversiones en el sector no solo para "asegurar la competitividad tecnológica a nivel mundial sino también para promover el desarrollo económico y social del país" (Alisson, 2018). En este sentido, es posible afirmar que los desafíos relativos a la falta de priorización en los programas de gobierno, las contingencias y recortes presupuestarios no son una exclusividad de la defensa nacional, sino que abarcan una amplia gama de sectores del país.

En segundo lugar, específicamente en lo que corresponde a la Ciencia Tecnología e Innovación de interés de la seguridad y defensa nacionales, el país no ha sacado provecho de los puntos fuertes y débiles específicos de su coyuntura.

Por un lado, el país está relativamente lejos de las grandes tensiones en términos de posibles conflictos internacionales. De igual forma, y aunque el estatus político-estratégico de un país como Brasil no le permita prescindir de sus Fuerzas Armadas, desde su entorno regional, el país actualmente no suscita mayores preocupaciones en relación con la emergencia de un conflicto internacional de naturaleza convencional en el corto y mediano plazo. Por otro lado, se observa que Brasil ha sido constantemente devastada por diversas crisis en el campo de la seguridad pública; esto ha llevado al Sector Defensa a desviar sus esfuerzos y encaminarlos hacia el fortalecimiento del rol de las Fuerzas Armadas y su participación en misiones de Garantía de la Ley y el Orden (GLO). La utilización de las Fuerzas Armadas para llenar los vacíos que existen en materia de seguridad pública no se presenta como una solución acorde a la complejidad y magnitud de este problema brasileño, el cual trasciende las dimensiones puramente militar y policial. Este uso inadecuado del más elevado instrumento militar a disposición

Fotografía: http://www.eb.mil.br/

del Estado en contra de la delincuencia sólo ha contribuido a desviar la atención de las Fuerzas Armadas, y aumentar su obsolescencia tecnológica y, sobre todo, organizacional frente a un escenario mundial inestable.

ALGUNOS DE LOS DESAFÍOS ACTUALES

A pesar de lo anterior, es necesario subrayar que algunas iniciativas importantes han tomado forma en los últimos años, incluso ante todas las dificultades, demostrando que los espacios para las innovaciones institucionales no sólo existen, sino que también pueden incrementar significativamente en el tiempo. Por ejemplo, el Plan de Apoyo Conjunto Inova Aerodefesa fue resultado de una suma de esfuerzos iniciados en 2013 entre la Empresa Brasileña de Innovación e Investigación (FINEP), el Banco Nacional de Desarrollo Económico y Social (BNDES), la Agencia Espacial Brasileña (AEB) y el Ministerio de Defensa. Este plan buscó apoyar proyectos en los sectores aeroespacial, de defensa y de seguridad con cerca de $2,9 mil millones, por medio de decretos públicos, combinando diversos instrumentos de financiación. Otra iniciativa para destacar es la creación, en 2016, del Sistema Defensa, Industria y Academia de Innovación (SISDIA), liderado por el Departamento de Ciencia y Tecnología (DCT) del Ejército Brasil, cuyo objetivo es identificar oportunidades asociadas entre el Ejército, la industria y centros de investigación.

Sin embargo, uno de los mayores desafíos observados tanto en el Inova Aerodefesa como en el SISDIA, por ejemplo, es la planificación y el poder de compra del gobierno en lo que se refiere a las adquisiciones de defensa, una vez que las soluciones y alianzas prospectivas difícilmente pueden traducirse en pedidos concretos. En esa dirección, es posible resaltar desafíos como (i) la falta de mecanismos claros de priorización de programas y proyectos entre las tres Fuerzas (Armada, Ejército y Fuerza Aérea); (ii) la débil articulación entre demandas tecnológicas en los campos de la inteligencia, defensa y seguridad pública, especialmente cuando se consideran las potencialidades de los sistemas de sistemas de comando y control (por ejemplo: Sistema de Vigilancia de la Amazonia - SIVAM - y los actuales Sistema Integrado de Monitoreo de Fronteras - SISFRON - y Sistema Integrado de Protección de Estructuras Críticas - PROTECT); y, finalmente, (iii) las discontinuidades de diversos proyectos y programas abarcados dentro de líneas tecnológicas específicas (ejemplo: área misilística y drones).

Fotografía: http://www.eb.mil.br/

> *[El] uso inadecuado del más elevado instrumento militar a disposición del Estado en contra de la delincuencia sólo ha contribuido a desviar la atención de las Fuerzas Armadas, y aumentar su obsolescencia tecnológica y, sobre todo, organizacional frente a un escenario mundial inestable.*

LA ARDUA Y NECESARIA BÚSQUEDA DE MECANISMOS DE PRIORIZACIÓN INTERINSTITUCIONAL

En este marco, y más allá del 1,5% del PIB asignado anualmente para la defensa nacional en Brasil, se encuentran otros caminos posibles para seguir avanzando en materia de tecnología; por ejemplo, analizar, estudiar y priorizar determinadas líneas tecnológicas que sean de interés común para distintos sectores, al menos, de los campos de inteligencia, defensa y seguridad pública. Al final, lo que está en juego es toda una gama de posibilidades de transformaciones sociales, políticas y culturales traídas a partir de un conjunto de nuevas tecnologías que trascienden al alcance solamente de la defensa nacional.

A manera de ejemplo, el gobierno canadiense definió dieciséis capacidades industriales claves (Key Industrial Capabilities - KICs), teniendo como foco el área de defensa (Canadá, 2018). En Brasil, la definición de tales líneas tecnológicas prioritarias podría auxiliar la viabilidad de diferentes proyectos y programas, orientando a largo plazo el nivel de prioridad de las iniciativas en el área de inteligencia, defensa y seguridad pública. Aquellas líneas tecnológicas prioritarias podrían utilizarse incluso como mecanismo para incentivar la conjuntez interagencial, dadas las posibilidades de aglutinar los recursos de adquisiciones, entrenamiento y operaciones en un solo proyecto como es el caso del Sistema Integrado de Monitoreo de Fronteras (SISFRON).

Fotografía: http://www.eb.mil.br/

"[LAS] LÍNEAS TECNOLÓGICAS PRIORITARIAS PODRÍAN UTILIZARSE INCLUSO COMO MECANISMO PARA **INCENTIVAR LA CONJUNTEZ INTERAGENCIAL**, DADAS LAS POSIBILIDADES DE AGLUTINAR LOS RECURSOS DE ADQUISICIONES, **ENTRENAMIENTO Y OPERACIONES** EN UN SOLO PROYECTO COMO ES EL CASO DEL **SISTEMA INTEGRADO DE MONITOREO DE FRONTERAS (SISFRON)."**

Fotografía: http://www.eb.mil.br/

BIBLIOGRAFÍA

Alisson, E. (7 de fevereiro de 2018). *Crise na ciência não se deve apenas à falta de recursos, avaliam cientistas.* Obtenido de http://agencia.fapesp.br/crise_na_ciencia_nao_se_deve_apenas_a_falta_de_recursos_avaliam_cienti stas/27103/ >. Acesso em: 05 Jun 2018.

Brimelow, B. (1 February de 2018). *It looks like China is about to test a futurist crailgun as the US Navy puts the brakes on its $500 million program.* Obtenido de http://www.businessinsider.com/china-testing-railgun-us-navy-2018-2

Deloitte. (08 2018 de Juny). Obtenido de Defense policy and the Internet of Things – disrupting global cyber defenses: https://www2.deloitte.com/jp/en/pages/public-sector/articles/gv/defensepolicy-and-the-internet-of-things.html

Deloitte. (08 June de 2018). Obtenido de Defense policy and the Internet of Things – disrupting global cyber defenses: https://www2.deloitte.com/jp/en/pages/public-sector/articles/gv/defensepolicy-and-the-internet-of-things.html

European Defense Agency. (18 December de 2017). Obtenido de EDA studies points towards Big Data potential for defence. Info hub. Latest News.: https://eda.europa.eu/info-hub/press-centre/latestnews/2017/12/18/eda-studies-points-towards-big-data-potential-for-defence

Freedberg Jr, S. (12 March de 2018). Obtenido de Marines' love affair with 3D printing: small is cheap, & beautiful. Defense News: https://breakingdefense.com/2018/03/marineslove- affair-with-3d-printing-small-is-cheap-beautiful/

Freedberg Jr, S. (14 October de 2016). Obtenido de US, UK do 'groundbreaking' drone exercise off Scotland. Breaking Defense: https://breakingdefense.com/2016/10/us-uk-dogroundbreaking- drone-exercise-off-scotland /

Insinna, V. (12 January de 2018). Obtenido de Russia's nuclear underwater drone is real and in the Nuclear Posture Review: https://www.defensenews.com/space/2018/01/12/russias-nuclear-underwater-drone-is-real-and-inthe- nuclear-posture-review/

Jennings, G. (03 November de 2016). Obtenido de UK prepares for Protector UAV. IHS Jane's Defence Weekly – Air Platforms,: http://www.janes.com/article/78529/uk-prepares-for-protector-uav

Kaspersen, A., Eide, E., Shetler Jones, P. (03 de November de 2016). Obtenido de 10 trends for the future of warfare. World Economic Forum: https://www.weforum.org/agenda/2016/11/the-4th-industrial-revolution-and-international-security

Knapp, B. (16 February de 2018). Obtenido de Here's where the Pentagon wants to invest in artificial intelligence in 2019. Defense News: https://www.defensenews.com/intelgeoint/ 2018/02/16/heres-where-the-pentagon-wants-to-invest-in-artificial-intelligence-in-2019/

Larter, D. (15 February de 2018). Obtenido de The Navy's stealth destroyers to get new weapons and a new mission: killing ships. Defense News: https://www.defensenews.com/naval/2018/02/15/its-official-the-navys-new-stealth-destroyers-willbe- ship-killers/

Martin, L. (08 June de 2018). Obtenido de Lockheed Martin receives $150 million contract to deliver integrated high energy laser weapon systems to U.S. Navy.: https://news.lockheedmartin.com/2018-03-01-Lockheed-Martin-Receives-150-Million-Contract-to- Deliver-Integrated-High-Energy-Laser-Weapon-Systems-to-U-S-Navy

Otan. (2016). Obtenido de Resilience: a core element of collective defence: https://www.nato.int/docu/review/2016/also-in- 2016/nato-defence-cyber-resilience/en/index.htm

Raytheon. (12 de November de 2017). Obtenido de To print a missile – Raytheon research points to 3-D printing for tomorrow's technology.: https://www.raytheon.com/index.php/news/feature/print-missile

Singer, P. (2009). *Wired for War.* NY: Penguin Books.

Peter Singer, E. B. (2018). *Like War: the weaponization of social media.* Eamon Dolan.

CRIMEN INTERNACIONAL Y SEGURIDAD AMBIENTAL, EL CASO DE LA AMAZONIA

Coronel Fábio Murilo

Coronel del Ejército de Brasil. Bachillerato en Ciencias Militares y Magíster en Operaciones Militares y en Ciencias Militares. Con experiencia en relaciones internacionales, crimen transnacional, seguridad fronteriza, seguridad y defensa nacionales. Investigador en el Centro Regional de Estudios Estratégicos en Seguridad, con foco de investigación en la temática de los crímenes transnacionales.

RESUMEN

La exuberancia de la selva amazónica llama la atención mundial. La región posee incontables riquezas minerales, abundantes depósitos de agua, gran potencial energético y un banco genético de dimensiones aún no completamente conocidas, pero que, sin duda, representa una nueva frontera para ser explotada por la ciencia. Evidentemente, toda esta abundancia atrajo la codicia humana y, en consecuencia, la Amazonia ha sido intensamente explotada, muchas veces de forma no sostenible e incluso ilegal, generando perjuicios económicos y ambientales gigantescos. El presente trabajo busca estudiar los principales delitos ambientales en curso en la Amazonía brasileña y sus impactos, así como presentar las medidas que vienen siendo adoptadas por el Estado brasileño para cohibir estas iniciativas criminales.

Palabras clave: *Amazonía, delitos ambientales, seguridad ambiental, crimen organizado*

ABSTRACT

The exuberance of the Amazon rainforest draws worldwide attention. The region possesses countless minerals, abundant water deposits, great energetic potential and a gene bank of dimensions not yet completely known, but that, without a doubt, represents a new frontier to be exploited by science. Evidently, all this abundance attracted human greed and, consequently, the Amazon has been intensely exploited, often unsustainably and even illegally, generating enormous economic and environmental damage. The present work seeks to study the main environmental crimes that underway the Brazilian Amazon and its impacts, as well as to present the measures that are being adopted by the Brazilian State to inhibit these criminal initiatives.

Keywords: *Amazon, environmental crimes, environmental security, organized crime*

INTRODUCCIÓN

La selva amazónica, con su exuberante flora y fauna y sus riquezas vírgenes, es una de las áreas más importantes del mundo para el futuro de la humanidad. Los estudios indican que alberga una de las más extraordinarias provincias minerales de la Tierra y su rica biodiversidad es vista como una potencial fuente de recursos para las industrias farmacéutica, bioquímica y agronómica, así como para muchas otras aplicaciones industriales.

Ferreira, Venticinque y Almeida destacan que la Amazonía se extiende desde el océano Atlántico a las laderas orientales de la Cordillera de los Andes, ocupando aproximadamente 7,8 millones de kilómetros cuadrados de la región centro-oriental de América del Sur: el 44% del territorio sudamericano (Ferreira, Venticinque e Almeida, 2005). Engloba áreas bajo nueve diferentes soberanías: Bolivia, Brasil, Colombia, Ecuador, Guyana, Guyana Francesa, Perú, Surinam y Venezuela.

En los últimos años la Amazonía viene siendo foco de la atención mundial. Temas como preservación y desarrollo sostenible han sido referencias constantes en conferencias, encuentros de Jefes de Estado e investigaciones científicas. El cambio climático y sus consecuencias, así como la escasez de recursos y la disputa por ellos están en la raíz de esta preocupación con la preservación de la Amazonía.

El concepto de preservación involucra diversas actividades que deben ser desarrolladas por el Estado, usando todas sus capacidades y con efectiva participación de la sociedad. Este rol de actividades va desde la seguridad en las fronteras hasta la prevención de la deforestación; de la lucha contra el crimen organizado a la construcción de infraestructura para integración regional; de ayuda a la población, salud, educación y ciudadanía al combate de la biopiratería.

Por sus inmensas potencialidades, la Amazonía está sujeta a diversas formas de explotación, no siempre legales. Sus dimensiones y características fisiográficas dificultan la actuación del Estado, creando oportunidades para la actuación del crimen transnacional, el cual, aprovechándose de las modificaciones introducidas por la globalización en los mercados, sistemas financieros, transportes y tecnología de la información, ha ampliado en las últimas décadas su penetración en la región.

“Por sus inmensas potencialidades, la Amazonía está sujeta a diversas formas de explotación, no siempre legales. Sus dimensiones y características fisiográficas dificultan la actuación del Estado, creando oportunidades para la actuación del crimen transnacional, el cual, aprovechándose de las modificaciones introducidas por la globalización en los mercados, sistemas financieros, transportes y tecnología de la información, ha ampliado en las últimas décadas su penetración en la región.”

1. AMAZONIA: CARACTERÍSTICAS, POTENCIAL Y DESAFÍOS

La importancia estratégica de la Amazonia y su influencia geopolítica pueden ser percibidas por la extensión de sus fronteras (11.000 km de fronteras terrestres y 1.600 km de frontera marítima) y por la buena navegabilidad de su cuenca hidrográfica, conectada al Océano Atlántico, permitiendo la interconexión de la región con las principales líneas de comunicaciones marítimas (Vidigal, 2002).

Al observar sus dimensiones y el porcentaje de territorio ocupado por la floresta se entiende la importancia de la Amazonia para Brasil. El área cubierta por la selva tropical, llamada en Brasil: Amazonia Legal, fue definida por la Cámara de Diputados en el año 2005 como:

> La región englobada por todos los estados de Acre, Amapá, Amazonas, Pará, Rondônia y Roraima y partes de Mato Grosso, Tocantins y Maranhão. La región abarca un área de aproximadamente 5.217.423 km², correspondiendo a cerca del 61% del territorio brasileño. Fue instituida con el objetivo de definir la delimitación geográfica de la región política captadora de incentivos fiscales con el propósito de promoción de su desarrollo regional

En términos de recursos minerales, la Amazonía tiene perspectivas vigorosas. Se estima que sus depósitos minerales acumulan recursos del orden de US$ 1,6 trillones (Lorencao, 2003), con variedad de yacimientos como hierro, manganeso, aluminio, cobre, zinc, níquel, cromo, titanio, fosfato, oro, plata, platino, paladio, rodio, estaño, tungsteno, niobio, tántalo, zirconio, tierras raras, uranio y diamantes.

En cuanto a la producción de petróleo y gas natural, la investigación en la región es reciente, pero las reservas actualmente mapeadas revelan un rico potencial, particularmente en la localidad de Coari.

La Amazonia también es un gran depósito de agua. La región posee cerca del 20% de todo el stock de agua dulce en la Tierra. Este gran volumen de agua, combinado con las características de los ríos, confieren la región más de 15.000 Km de hidrovías con más de dos metros de profundidad incluso en la estación seca. Por otro lado, la región también tiene gran potencial para generar electricidad. En

Fotografía: http://www.eb.mil.br/

la investigación anterior, que no cubre toda la capacidad existente, la región puede tener más de 120.000 megavatios (mw), un potencial mayor que la capacidad instalada de todas las centrales hidroeléctricas de Estados Unidos (115.000 mw) (Viana-Sampaio, 2011).

La biodiversidad es el factor más relevante en la importancia ambiental de la Amazonía. Un tercio de las especies del planeta viven allí, es decir, cerca del 30% de todas las secuencias de ADN de la Tierra. En cuanto a las reservas de madera del Amazonas, el valor económico es aproximadamente de US$ 1.7 trillón (Lorencao, 2003).

El gran desafío es hacer uso racional de estos recursos, integrando la región y su población al resto del país sin degradar su mayor riqueza: el propio bosque. Las presiones son inmensas y variadas: agronegocios, minería, hidroeléctricas, además de las diversas amenazas representadas por el crimen transnacional.

La preocupación por generar una capacidad económica bajo una percepción de preservación ambiental pasa a ser un punto focal cuando se trata de la Amazonia, un ecosistema que, por sus dimensiones y exuberancia, afecta profundamente la seguridad ambiental de la humanidad.

El concepto de seguridad ambiental surge de la preocupación por mantener las condiciones de vida en un planeta donde la explotación económica de la naturaleza nos viene llevando a la escasez de recursos y, en algunos casos, a una exacerbada disputa por el acoso a ellos.

En la Amazonia, esta disputa abre espacio para que agentes inescrupulosos busquen mantener sus ganancias financieras independiente de las obligaciones y restricciones impuestas por la ley. Los grandes beneficios involucrados en algunas de estas actividades exploratorias atrae a organizaciones criminales transnacionales que perciben en las dificultades de control impuestas por las características amazónicas un factor de protección.

2. EL CRIMEN ORGANIZADO TRANSNACIONAL (COT) Y LOS DELITOS AMBIENTALES EN LA AMAZONIA

Hay varias modalidades del crimen transnacional presentes en la Amazonia. La más visible y divulgada es el tráfico de drogas, en especial de cocaína, que utiliza los diversos ríos de la región como ruta de abastecimiento de sus cadenas logísticas y acceso a sus mercados consumidores, además de aprovechar la cobertura del bosque para instalar laboratorios de producción o refino. En lo que se refiere a la seguridad ambiental, la presencia de esta actividad representa una amenaza importante, por la posibilidad de contaminación química de la red hidrográfica del área con rechazos y descartes de la producción. Otra cuestión ambiental planteada por la temática del tráfico de drogas es la contaminación fluvial por agentes químicos usados como herramientas para erradicar los plantíos ilegales de coca.

“En la Amazonia, esta disputa abre espacio para que agentes inescrupulosos busquen mantener sus ganancias financieras independiente de las obligaciones y restricciones impuestas por la ley. Los grandes beneficios involucrados en algunas de estas actividades exploratorias atrae a organizaciones criminales transnacionales que perciben en las dificultades de control impuestas por las características amazónicas un factor de protección.”

Fuente: Valter Campanato/Agencia Brasil

Laboratorio de refino de cocaína en la Amazonia brasileña: Vista aérea del laboratorio de refino de cocaína, descubierto en operación conjunta del Ejército y de la Policía Civil del Amazonas

"EL MAYOR PERJUICIO AL MEDIO AMBIENTE NO ES CAUSADO POR LAS EMPRESAS MINERAS, **ES GENERADO POR LA MINERÍA ILEGAL**, QUE, ADEMÁS DE NO SUFRIR LAS **RESTRICCIONES AMBIENTALES Y NORMATIVAS** A QUE SE SOMETEN LAS EMPRESAS MINERAS, USAN **TÉCNICAS DE PROSPECCIÓN ATRASADAS Y ALTAMENTE CONTAMINANTES."**

Otra relevante amenaza a la seguridad ambiental amazónica es representada por la minería. Es un riesgo por la destrucción de la cobertura vegetal, con consecuentes daños a la biodiversidad y también por el tratamiento dado a los desechos, de gran potencial contaminante. Como se trata de una modalidad donde los beneficios son significativos, la capacidad de generar corrupción en agentes gubernamentales responsables de las autorizaciones ambientales y fiscalizaciones de funcionamiento de la actividad también se convierte en una amenaza.

Sin embargo, el mayor perjuicio al medio ambiente no es causado por las empresas mineras, es generado por la minería ilegal, que, además de no sufrir las restricciones ambientales y normativas a que se someten las empresas mineras, usan técnicas de prospección atrasadas y altamente contaminantes. Un buen ejemplo de esto es el uso de mercurio en los *garimpos*[2] ilegales de oro, esparcidos por diversos puntos de la Amazonia, que es desechado en los ríos, generando diversos problemas de salud en las poblaciones ribereñas además de incalculables daños a la fauna y a la flora. En cuanto a los ríos, algunas técnicas utilizadas llevan a su sedimentación, reduciendo su volumen de agua, con pérdidas significativas al equilibrio ambiental.

Muchos otros problemas se asocian a la minería ilegal, entre ellos el tráfico de drogas, la prostitución, la evasión de divisas y el lavado de dinero. Un factor preocupante es la invasión, por parte de *garimperos*[3] ilegales, de reservas indígenas, parques forestales y otras áreas de preservación ambiental, lo que, de acuerdo con la legislación brasileña, puede ser encuadrado criminalmente.

[1] Término en portugués usado para referirse a la excavaciones producto de la actividad extractiva.

[2] Término en portugués usado para referirse a las personas dedicadas a la actividad extractiva.

Fotografía: http://www.eb.mil.br/

En el caso particular del oro y del diamante, como su origen es difícil de definir y poseen alto valor de mercado, hay una tendencia de utilización para el lavado de dinero por parte de organizaciones vinculadas al narcotráfico.

La venta de animales silvestres es otra modalidad de crimen ambiental transnacional encontrada en la Amazonia. Las especies nativas llegan a ser comercializadas por altas sumas, siendo adquiridas por coleccionistas de diversas partes del mundo e incluso por instituciones de investigación para los más diversos tipos de estudios. Además del comercio, algunos animales también son sacrificados para el comercio de su carne o piel.

El enorme potencial genético de la selva amazónica también atrae la codicia del crimen organizado. El Instituto Brasileño del Medio Ambiente (IBAMA) define esta apropiación indebida de recursos de la biodiversidad para uso científico o biotecnológico como biopiratería. A fin de permitir la investigación científica, en 2015 Brasil creó reglas para la remisión de patrimonio genético al exterior con finalidades científicas o de desarrollo tecnológico; sin embargo, la industria internacional aún ha buscado alternativas que le permita burlar las imposiciones legales brasileñas.

A pesar de todos los fenómenos mencionados anteriormente, el problema de mayor visibilidad en la Amazonia, y que llama la atención de la comunidad mundial, es la deforestación. Numerosas son las presiones sobre la cobertura vegetal de la región, pero una dinámica fácilmente perceptible es el avance de las áreas de agricultura y ganadería sobre el bosque.

Hay un estándar en esta dinámica. Se procesa de sur a norte, creando el llamado arco de la deforestación: una banda de territorio que abarca partes de Rondônia y Acre, el norte de Mato Grosso y el sur de Pará. Esta es el área con la tasa más alta de deforestación.

La cobertura natural se retira para la formación de pastos y para la agricultura familiar. En seguida, estas áreas se pasan a empresas agrícolas y ceden sus espacios a las grandes plantaciones, de alto uso de tecnología y mecanización, mientras los agricultores siguen hacia el norte iniciando un nuevo ciclo de deforestación.

La madera retirada en este proceso es vendida a las madereras, generalmente sin los debidos sellos de autorización de corte y transporte o, muchas veces con documentos regulatorios falsos u obtenidos por medio de corrupción.

Fuente: Divulgação/IBAMA

Apreciación de troncos de madera extraídos ilegalmente, en la región del río Javari.

Hay informes, además, de la utilización de mano de obra indígena. Algunos madereros, ligados al crimen transnacional, estarían obligando a las comunidades a hacer el corte de madera y venderla adentro y fuera de Brasil. Escada et al (2005) también asocia el corte de madera en reservas indígenas con la convivencia y hasta la participación de estos.

3. EL ESTADO BRASILEÑO EN EL COMBATE AL COT EN LA AMAZONIA

Frente a tantas amenazas, el Estado brasileño no podría quedar inerte. Numerosas iniciativas de combate al crimen ambiental y de preservación y protección de la Amazonía están actualmente en curso, con la participación de los diversos entes estatales. El Programa de Protección Integrada de Fronteras, lanzado en 2016, es hoy el marco legal que baliza esta actuación, teniendo como directrices la acción integrada y coordinada de los órganos de seguridad e inteligencia y la cooperación e integración con los países vecinos (Gabinete de Segurança Institucional, 2018).

El Sistema de Protección de la Amazonía es una de estas iniciativas. Utiliza datos generados por una infraestructura tecnológica, compuesta por subsistemas integrados de sensores remotos, radares, estaciones meteorológicas y plataformas de recolección de datos, instaladas en la región amazónica, para promover el completo monitoreo de la región y producir informaciones en tiempo próximo al real.

El sistema realiza la recolección de datos, almacenamiento y tratamiento de informaciones, permitiendo el funcionamiento articulado e integrado de las diversas instituciones gubernamentales en el control de las deforestación; en el combate a la biopiratería; en la protección de las unidades de conservación; en el monitoreo de la ocupación y uso del suelo; en la protección de las reservas indígenas; en la defensa de las zonas fronterizas; en la protección de los recursos minerales estratégicos; y en la implementación de programas de salud, educación e inclusión social para las poblaciones amazónicas.

Fotografía: http://www.eb.mil.br/

OPERACIÓN ÁGATA

La Operación Ágata es de responsabilidad del Ministerio de Defensa, bajo la coordinación del Estado Mayor Conjunto de las Fuerzas Armadas (EMCFA), junto con el Ejército, Marina y Aeronáutica. La operación, en el marco del Plan Estratégico de Fronteras, tiene por objetivo intensificar la presencia del Estado brasileño ante la franja de frontera, contribuyendo al combate y la reducción de ilícitos como contrabando, tráfico de drogas, de personas, de armas y municiones, explotación sexual, evasión de divisas, delitos ambientales, robo de vehículos, minería ilegal, entre otros.

Las acciones tácticas desencadenadas durante las Operaciones Ágata van desde vigilancia del espacio aéreo al patrullaje e inspección en los principales ríos y carreteras que dan acceso al país.

Mientras las Operaciones Ágata, de carácter puntual y temporal, se destacan por la fuerte participación del componente militar actuando en puntos focales de la franja de frontera bajo la coordinación del Ministerio de Defensa, las Operaciones Centinela, de carácter sistemático y permanente, concentran su esfuerzo en las líneas de investigación e inteligencia y en la actuación conjunta de los mecanismos federales de seguridad (Policía Federal, Policía Federal de Tránsito y Fuerza Nacional de Seguridad) bajo la coordinación del Ministerio de Justicia.

Con más de 16.000 kilómetros de frontera (Ministério da Defesa, 2019), la presencia física en todos los puntos es una imposibilidad. Con esta premisa en mente y buscando una actuación de seguridad, protección y vigilancia efectiva, se desarrolló el Sistema Integrado de Monitoreo de Fronteras (SISFRON).

Los primeros pasos del programa fueron dados en 2012, con una iniciativa del Ejército. El sistema prevé la utilización de la moderna tecnología para integrar sensores -como de sistemas de vigilancia, imágenes por satélites, vehículos aéreos no tripulados y radares - y actuadores, es decir, la tropa dispuesta en el terreno, la cual se dará la necesaria movilidad para actuar en un corto espacio de tiempo, en una franja de frontera de distancias continentales.

"CON MÁS DE **16.000 KILÓMETROS DE FRONTERA** (MINISTÉRIO DA DEFESA, 2019), LA PRESENCIA **FÍSICA EN TODOS LOS PUNTOS** ES UNA IMPOSIBILIDAD. CON ESTA PREMISA EN MENTE Y BUSCANDO U**NA ACTUACIÓN DE SEGURIDAD, PROTECCIÓN Y VIGILANCIA EFECTIVA,** SE DESARROLLÓ EL SISTEMA INTEGRADO DE MONITOREO DE FRONTERAS **(SISFRON)."**

De acuerdo con el antiguo Comandante del Ejército, Gen Enzo Peri (2011), el SISFRON va a aumentar la presencia del Estado en la Amazonia. Busca promover la integración regional, estimular la cooperación militar con los países vecinos, ayudar en la preservación de la región amazónica y la protección de la biodiversidad, combatir ilícitos ambientales y deforestación, proteger a las poblaciones indígenas y aumentar la sensación de seguridad en el área, ya que va a actuar contra todo tipo de crímenes comunes en nuestras regiones fronterizas.

Las Fuerzas Armadas en diversos lugares de la Amazonia brasileña representan la única manifestación de la presencia del Estado. No podrían, por lo tanto, quedar ajenas a las acciones de combate a los delitos ambientales cometidos por el crimen organizado transnacional. Además de las operaciones y programas ya mencionados, el componente militar, que, por lo previsto en el ordenamiento jurídico brasileño, posee poder de policía en una franja de 150 Km del territorio nacional, a partir de la franja de

frontera, desencadena, diuturnamente, operaciones con sus medios orgánicos para combatir los diversos crímenes ambientales en la región.

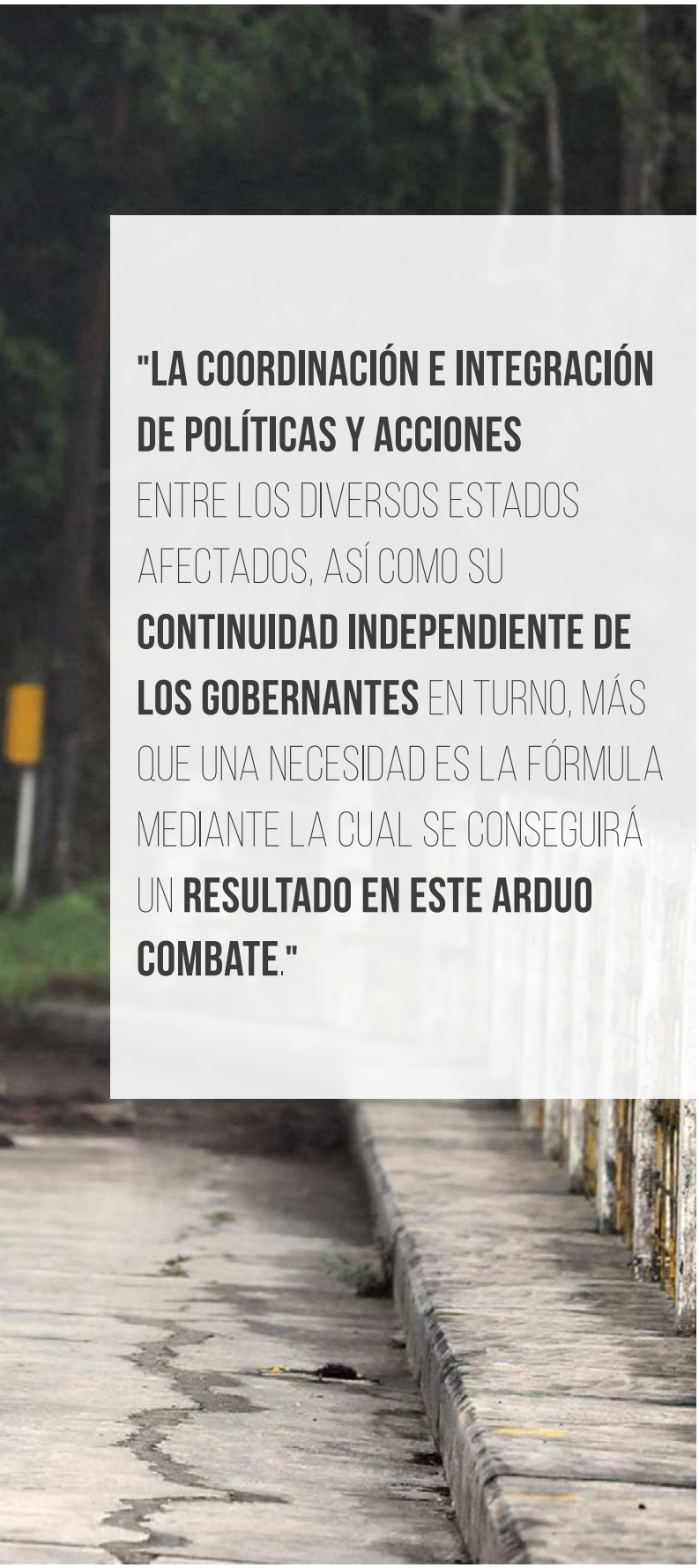
Se destacan las operaciones con el IBAMA y el Instituto Chico Mendes de Conservación de la Biodiversidad (ICMBio) en el combate a la minería ilegal y la deforestación y el patrullaje y fiscalización de embarcaciones en los principales ríos de la región, así como el apoyo en comunicaciones, inteligencia y logística para permitir que los diversos entes estatales con atribuciones de fiscalización ambiental o de combate al crimen, en sus diversas modalidades, puedan actuar en la región.

A propósito, cabe destacar que el transporte fluvial de drogas sufrió un aumento significativo a partir de 2004, cuando se reguló la ley que autoriza derribar aeronaves sospechosas de involucrarse con el tráfico de estupefacientes (Lima, 2018).

Lima (2018) explica que, una vez identificada una aeronave sospechosa, se aplicarán gradualmente las medidas coercitivas de investigación, intervención y persuasión. Si no hay respuesta de carácter práctico por parte de la tripulación de la aeronave interceptada, en el sentido de realizar el aterrizaje para obediencia a las medidas de control en el suelo, los procedimientos de derribar entrarán en curso. Evidentemente, por la sensibilidad del tema, la decisión de derribar debe ser tomada en el más alto escalón.

Pese al cuestionamiento de algunos investigadores en cuanto a la efectividad de la ley se nota, a partir de su promulgación, un cambio en el modo de actuación del narcotráfico en la región, el cual pasó a intensificar la utilización de modalidades fluviales y terrestres, en detrimento del aéreo, y a buscar nuevas rutas para acceder al territorio brasileño.

Fotografía: http://www.eb.mil.br/



"LA COORDINACIÓN E INTEGRACIÓN DE POLÍTICAS Y ACCIONES ENTRE LOS DIVERSOS ESTADOS AFECTADOS, ASÍ COMO SU **CONTINUIDAD INDEPENDIENTE DE LOS GOBERNANTES** EN TURNO, MÁS QUE UNA NECESIDAD ES LA FÓRMULA MEDIANTE LA CUAL SE CONSEGUIRÁ UN **RESULTADO EN ESTE ARDUO COMBATE**."

III. CONCLUSIONES

El crimen organizado transnacional, en sus diversas modalidades, no considera los límites territoriales impuestos por las soberanías de los diversos países. Para que se pueda combatirlo con efectividad se hace necesario extrapolar estas líneas de frontera. La coordinación e integración de políticas y acciones entre los diversos Estados afectados, así como su continuidad independiente de los gobernantes en turno, más que una necesidad es la fórmula mediante la cual se conseguirá un resultado en este arduo combate.

Las características fisiográficas de la Amazonía dificultan la presencia del Estado. Integrar la región, trayendo a la población local los servicios y beneficios disponibles para el ciudadano de las demás partes del país y buscar arreglos productivos locales que, respetando las peculiaridades de cada comunidad, permitan una explotación económica sostenible de las riquezas del bosque, más que un anhelo, es una obligación del Estado brasileño que, en la medida en que sea exitoso en esta empresa, estará imponiendo un vigoroso revés a las actividades ilícitas en el área.

La certeza de la ley es una de las grandes fuerzas de la sociedad. Al intensificar su presencia, sea por medio de operaciones sistemáticas o eventuales de sus órganos de seguridad, sea por medio de programas, reglamentación y fiscalización por parte de sus vehículos de protección ambiental y fiscal, y por la judicialización y condena de conductas irregulares o criminales, la región conquistará resultados expresivos en la lucha contra la criminalidad transnacional.

La amenaza a la sociedad, representada por el crimen organizado transnacional, no es sólo un problema policial, es un riesgo para la soberanía y el funcionamiento del Estado. Por lo tanto, sólo un enfoque amplio con la participación efectiva de todas las capacidades del Estado logrará obtener éxito contra este flagelo que asola a la humanidad en el alba del siglo XXI, en especial en una región de tanta importancia para el futuro de las condiciones de supervivencia en nuestro planeta.

BIBLIOGRAFÍA

1. Câmara dos Deputados do Brasil. (2005). *Amazônia Legal*. Recuperado de https://www2.camara.leg.br/camaranoticias/noticias/70447.html

2. Centro Gestor e Operacional do Sistema de Proteção da Amazônia. (2015). *Relatório de Atividades 2015*. Recuperado de http://www.sipam.gov.br/sobre/arquivos/relatorios/relatorio-de-atividades-2015.pdf

3. Collins, A. (2007). *Contemporary Security Studies*. Oxford, Reino Unido: Oxford University Press.

4. Escada, M. I. S., Vieira, I. C. G., Kampel, S. A., Araújo, R., Da Veiga, J. B., Aguiar, A. P. D., … Câmara, G. (2005). Processos de ocupação nas novas fronteiras da Amazônia (o interflúvio do Xingu/ Iriri). *Estudos Avançados 19* (54), 09-23.

5. Ferreira, L.V., Venticinque, E., Almeida, S. (2005). O desmatamento da Amazonia e a importância das áreas protegidas. *Estudos Avançados*, *19* (53), 157-166.

6. Gabinete de Segurança Institucional. (2018). *Programa de Proteção Integrada de Fronteiras*. Recuperado de http://gsi.gov.br/arquivos/ppif.pdf.

7. Instituto Brasileiro do Meio Ambiente e dos Recursos Naturais Renováveis. (2016). *Francesa é detida em Guarulhos (SP) ao tentar embarcar com animais silvestres na bagagem*. Recuperado de http://www.ibama.gov.br/component/tags/tag/biopirataria

8. Lima, I. Z. L. (2018). A lei do abate no combate ao narcotráfico: essencial ou inconstitucional?. *Âmbito Jurídico, XXI* (170). Recuperado de http://www.ambito-juridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=20298&revista_caderno=9.

9. Lorenção, J. H. (2003). *A Defesa Nacional e a Amazônia: o Sistema de Vigilância da Amazônia*. (tese de mestrado em Ciências Políticas). Unicamp, Campinas, Brasil.

10. Ministério da Defesa. (2019). *Proteção das Fronteiras*. Recuperado de https://www.defesa.gov.br/exercicios-e-operacoes/protecao-das-fronteiras

11. PERIN, O. (2011). Sisfron: Gen Enzo apresenta o sistema. *Defesanet*. Recuperado de http://goo.gl/S2M572

12. Santos, B. A. (1998). Recursos Minerais da Amazônia. Em Freitas, M. L. D. (Ed.), *Amazonia – Heaven of a New World* (pp. 111-126). Rio de janeiro, Brasil. Editora Campos

13. Viana-Sampaio,F. M., (2011). *Protection of the Amazon: the Role of the Army.* (tesis de posgrado). Joint Services Command and Staff College, Shrivenham, Reino Unido.

14. Vidigal, A. A. F. (2002). A internacionalização da Amazônia. *Revista Marítima Brasileira. Volume* (122), 81-99.

Fotografía: http://www.eb.mil.br/

SECURITY SECTOR REFORM: KOSOVO'S EXPERIENCE

Bilbil Kastrati

MA Bilbil Kastrati, PhD student in Security Studies, University of Ljubljana, Slovenia, email: bilbil.kastrati@student.uni-lj.si / bilbil.kastrati@gmail.com

ABSTRACT

Security Sector Reform (SSR) is a process that aims to identify security threats to a state or society and to establish good governance security sector under civilian oversight, which is accountable and can protect effectively the citizens. This article aims to analyse the Kosovo SSR in two time periods in 2006 and 2014. It elaborates the security threats to Kosovo and its citizens, and describes the measures introduced to counteract these threats. Furthermore, the article focuses on comparing the advantages and disadvantages in conducting internationally and locally driven SSR. It will highlight the necessity for inclusion in the SSR process of all affected parties and avoiding the limitation of the SSR only to security institutions. The article concludes that Kosovo's experience shows that locally driven SSR are more limited than those internationally driven; and that inclusion of specialized organizations such as United Nations or European Union ensures comprehensive SSR that identifies security threats towards both state institutions and citizens; and provides inclusive and practical solutions on how to deter these threats. And, finally the lesson learned from Kosovo is that there is little worth of having a developed and efficient security sector if the population of the country is ill-educated, unemployed and unhealthy, vulnerable to drugs, trafficking, extremism, etc.

Keywords: *Kosovo, SSR, ISSR, SSSR*

REFORMA AL SECTOR DE SEGURIDAD: LA EXPERIENCIA DE KOSOVO

RESUMEN

La Reforma del Sector de Seguridad (SSR, por sus siglas en inglés) es un proceso que tiene como objetivo identificar amenazas de seguridad para un estado o sociedad y establecer una buena gobernanza en el sector de seguridad bajo supervisión civil, que es responsable y puede proteger eficazmente a los ciudadanos. Este artículo pretende analizar la RSS de Kosovo en dos períodos de tiempo en 2006 y 2014. Aborda las amenazas de seguridad para Kosovo y sus ciudadanos, y describe las medidas introducidas para contrarrestar estas amenazas. Además, el artículo se centra en comparar las ventajas y desventajas de la conducción de SSR a nivel internacional y local. Destacará la necesidad de incluir en el proceso de SSR de todas las partes afectadas y evitará la limitación del SSR solo a las instituciones de seguridad. El artículo concluye que la experiencia de Kosovo muestra que la RSS localmente es más limitada que la internacional; y que la inclusión de organizaciones especializadas como las Naciones Unidas o la Unión Europea garantiza una SSR integral que identifique amenazas de seguridad tanto para las instituciones estatales como para los ciudadanos; y proporciona soluciones inclusivas y prácticas sobre cómo disuadir estas amenazas. Finalmente, la lección aprendida de Kosovo es que hay poco valor al tener un sector de seguridad desarrollado y eficiente si la población del país es mal educada, desempleada e insalubre, vulnerable a las drogas, el tráfico, el extremismo, etc.

Palabras clave: *Kosovo, RSS, RISS, RESS*

INTRODUCCIÓN

Kosovo is a small south-eastern European country with a population of less than two million. Its resent history was troubled. Namely, Kosovo was announced an independent state on 17 February 2008, and it is result of dissolution of the former state of Yugoslavia[1]. However, Kosovo is not recognized by Serbia from who was separated and still is not member either of United Nations (UN) or European Union (EU) and other regional or world organizations[2]. Kosovo, a former province of Yugoslavia (Serbia) with majority population of ethnic Albanians, was struggling during late '80s and early '90s for its autonomy which was suspended by Serbia in 1989. Kosovo Albanians reacted in Serbia's action peacefully establishing a movement[3] in early '90s which was seeking a peaceful agreement with Serbs. Since no peaceful agreement was reached, in late '90s the Albanian hardliners resort to arms and guerrilla formation – Kosovo Liberation Army (KLA) - attacked the Serbian Security Forces which prompted harsh reaction of the latter against Albanian civilian population[4]. The international community lead by European's, American's and Russian's made an attempt in early '99 in France[5] to mediate a solution of the conflict and to end the hostilities between Serbians and Albanians. However, since the Serbian side refused to sign a peace agreement and with the deteriorating circumstances in the field in Kosovo as a result of fierce attacks of Serbian Security Forces in civilian population, the international community[6] could not stand indifferent and as a result the North Atlantic Treaty Organization (NATO) launched a military attack against Serbia which lasted for 78 days and defeated the Serbian Security Forces which had to withdraw from Kosovo[7]. Following this event the United Nations Security Council adopted Resolution 1244, on 10 June 1999 which set Kosovo under its protectorate through United Nations Interim Administration Mission in Kosovo (UNMIK) (United Nations Security Council, 1999).

[1] Other states that came after dissolution of Yugoslavia are: Slovenia (EU), Croatia (EU), Serbia, Bosnia and Herzegovina, Montenegro and Northern Macedonia.

[2] Kosovo is member of the World Band, International Monetary Fund, UEFA and 20 other regional and international organizations.

[3] Democratic Leagues of Kosovo – lead by Dr Ibrahim Rugova.

[4] Kosovo war 1998-99 resulted with over 10,000 civilian victims and massive forceful deportation of Albanians from Kosovo which by mid-'99 reach almost 1 million refugees. See: Kosovo refugee crisis: An independent evaluation of UNHCR's emergency preparedness and response.

[5] 'Rambouillet Accords' signed by Kosovo delegation, but refused to be signed by Serbian delegation.

[6] Western European countries' and America, and informally blessed by Russia.

[7] Military technical agreement between the international security force (KFOR) and the Government of the Federal Republic of Yugoslavia and the Republic of Serbia.

INCEPTION AND DEVELOPMENT OF THE SSR IN KOSOVO

Since 1999 the UN has been the primary security provider for Kosovo[8]. Through Resolution 1244 the UN requested demilitarization of the KLA after cessations of hostilities with Serbian Security Forces. Demilitarization of the KLA and its transformation into Kosovo Protection Corps (KPC) was the first step in security sector reform of Kosovo as a separate entity under international oversight[9]. Parallel to demilitarization of the KLA, the process of establishing a new Kosovo Police force in 1999 was underway. This process was led by the Organization for Security and Cooperation in Europe (OSCE)[10].

While Kosovo was developing its governance, rule of law and security institutions; political environment due to unsettled political status of Kosovo raised security tensions. In 2004, huge riots and clashes between communities in Kosovo (Albanians and Serbians) and against the international community erupted[11]. As a result UN sent an envoy Kai Eide to do an assessment of the situation. On 30 November 2004, Eide submitted a report to UN Secretary General with recommendations suggesting further reforms for Kosovo and its status settlement (United Nations Security Council, 2004). In light of this, in 2005 the head of UNMIK initiated the Internal Security Sector Review (ISSR) in Kosovo.

ISSR

The SSR is crucial for understanding the effects of changes in the security sector and in establishing the overall reform of the governmental institutions. Kosovo is a unique example in the world where a holistic review was conducted prior

[8] Kosovo Force - KFOR- is the responsible international security component that provides hard security for Kosovo.

[9] Through this transformation a military guerrilla group KLA was transformed to a civilian emergency service agency the KPC. While the KLA had some 16,000 soldiers , the KPC consisted of 3,000 active members and 2,000 reserve members.

[10] Transformation of the KLA and establishing the Kosovo Police processes were the nucleus of the SSR in Kosovo, although at a limited level and without proper analysis.

[11] As a consequence of this turmoil 27 citizens of Kosovo were killed.

"ISSR KOSOVO WAS A CONSULTATIVE PROCESS, WITH **EXTENDED OUTREACH TO THE PUBLIC** THAT AIMED TO DEFINE **SECURITY FOR PEOPLE** OF KOSOVO, AS WELL AS AN ANALYSIS OF CURRENT SECURITY THREATS AND **INSTITUTIONAL CAPACITY GAP TO ADDRESS** THOSE THREATS, AND **OTHER OF THE FUTURE."**

to security sector engagement. ISSR Kosovo was a consultative process, with extended outreach to the public that aimed to define security for people of Kosovo, as well as an analysis of current security threats and institutional capacity gap to address those threats, and other of the future. This was the first time such an approach was adopted since often the SSR's are limited either by methodology or scope and are conducted internally within security institutions such as military, police or intelligence services, without or with limited public consultation. The ISSR methodology involved two key concepts, first the analysis of the perceived threats based on public outreach and consultation with Kosovo institutions; and second, using the Copenhagen Criteria (1993)[12] as a benchmark to measure results. In this context, the ISSR assessed the internal security threats stemming from political, economic and social aspects; as well as the external security threats. The research has identified three main internal threats for Kosovo:

- Economic insecurity,
- Weak rule of law, and
- Political instability.

Further, some other not frequent security threats were identified: violence against women, organized crime, threats to environment, trafficking in human beings and inadequate public services. While other major perceived threats include: freedom of movement, unemployment, ethnic violence, terrorism, corruption, drugs, diseases and poverty. External threats to Kosovo are linked mainly to the neighbouring relations, particularly with Serbia due to the future settlement of the political status of Kosovo, which may insight political violence between Serbs and Albanians within Kosovo;

[12]Copenhagen Criteria foresee that states aspiring EU accession should have: stable institutions guaranteeing democracy, the rule of law, human rights and respect for minorities; functioning of a market economy and incorporation of the EU law into domestic legislation, as a necessary benchmark for development of institutions and formulation of the security policy.

> *Economy and unemployment were the key issues that raised fear for job security, growing poverty that insight crime and corruption in Kosovo. Therefore, ISSR recommended that Kosovo implements effective economic policies and instructed to create favourable business environment, attract foreign investment and to generate employment and to include in the economic processes disadvantaged groups.*

and potentially a cross-border insurgency. ISSR has devoted particular attention to the security concerns of the vulnerable and under-represented groups of the society women and youth, as well as other marginalized communities[13]. ISSR has looked at functioning of the actors that do not provide directly security to Kosovo citizens[14] as well as the functional analysis of security institutions of Kosovo[15].

ISSR has made a number of recommendations to address the key security threats, bridging of the institutional gaps and has proposed the new security architecture of Kosovo.

- **Economy.** Economy and unemployment were the key issues that raised fear for job security, growing poverty that insight crime and corruption in Kosovo. Therefore, ISSR recommended that Kosovo implements effective economic policies and instructed to create favourable business environment, attract foreign investment and to generate employment and to include in the economic processes disadvantaged groups.

- **Health.** Kosovo had no health security schemes established at state level and suffers from lack of formalized emergency procedures in the area of health care. It was recommended that mechanisms are established to monitor security risks such as epidemics.

- **Education.** There is a significant gap in access to information, educational curriculum and teaching methods. It was recommended that Kosovo curricula especially in higher education should be reviewed. Further, Kosovo should extend their cooperation with regional and other external universities in order to provide for more opportunities for youth to enhance their skills.

- **Governance institutions.** Kosovo should focus its attention across all institutional structures those directly responsible for security and other to improve their capacities, develop modern polices and legislation compliant with EU standards, ensure oversight of civilian authority over security sector, increase the trust between citizens and governance institutions, as well as to open more for further regional cooperation.

- **Security architecture.** ISSR has proposed new security architecture for Kosovo as part of its institutional development and awaiting its final political status resolution. This would include: Kosovo Security Council, Ministry of Defence, Ministry of Internal Affairs, Ministry of Justice, Ministry of Finance and Economy, Kosovo Defence Force, Kosovo Police Service, Security Service and the Department of Emergency Management; and Assembly committees for defence and security service.

Of note, the UN efforts to reach a political settlement for Kosovo's final political status failed in 2007. Martti Ahtisaari, the UN Secretary General envoy, proposed a conditional independence for Kosovo in March 2007 (United Nations Security Council, 2007), however, since the Security Council members had disagreements over this proposal, especially with opposition of the Russian Federation; the proposal was never put forward for voting in the Council. Nevertheless, Kosovo unilaterally accepted the proposal for conditional independence and incorporated Ahtisaari's requirements into its political and constitutional life

[13] All these three vulnerable communities women and youth, as well as other marginalized communities for example suffer from lack of adequate education, unemployment, are excluded from political processes and decision making which makes them vulnerable towards organized crime, infiltration in the drug trade and terrorism.

[14] ISSR concluded that issues such as trade, energy, health, education all play a role on how safe Kosovo citizens feel in their homes.

[15] Crisis and Emergency Management, Kosovo Police Service, Kosovo Protection Corps, Kosovo Correctional Service, Border Control, as well as non-institutional security related subjects such as Small Arms and Lights Weapons and Private Security Companies.

and declared its independence on 17 February 2008. In terms of the security institutions, since Kosovo agreed to have a conditional independence (lasted until 2012), some adjustments had to be made in the terminology and functioning of these institutions. For example, Kosovo Defence Force was renamed Kosovo Security Force without defence authorizations, focusing mainly on the rapid reaction forces. The Defence Ministry was labelled Ministry of the Kosovo Security Force. While the Security Service was named Kosovo Intelligence Agency.

STRATEGIC SECURITY SECTOR REFORM (SSSR)

In 2012 the Government of Kosovo has initiated the SSSR that was completed in 2014 (Republic of Kosovo, 2014)[16]. The SSSR aim was to perform a comprehensive analysis of all security aspects of Kosovo to identify and analyse current and future security threats; to establish roles of each security institution to ensure maximal institutional output; and to identify required capabilities build-up to guarantee safe and secure environment for all Kosovo's citizens. SSSR in Kosovo is the first post-independence SSR which emphasised the local ownership and had the objective to establish effective, efficient and accountable security sector in Kosovo.

The SSSR has reviewed the roles and responsibilities, missions and legal bases of the security sector institutions and has recommended changes of the roles and missions of these institutions with focus on transformation of the Kosovo Security Force into Kosovo Armed Forces and transition of the Ministry for Kosovo Security Force into Ministry of Defence (Kosovo Ministry of Defence, 2019). Furthermore, the SSSR has suggested that some security institutions should be dissolved while new ones should be established, and that further capacity building of the current security institutions is needed. In order, to bring to live all these changes legislative and policy reforms were recommended. On a separate note, the SSSR is claimed to be transparent and open for the public and that the civil society has validated the SSSR process[17].

The SSSR has analysed the international, regional and internal security environment and threats to Kosovo.

[16] The Inter-ministerial Working Group that conducted SSSR was composed of: Kosovo Security Force (KSF), police and the intelligence services; ministries of KSF, foreign affairs, interior, justice, finance, environment, infrastructure, health and education.

[17] The main objectives of the SSSR were: To define Strategic Objectives of Kosovo and Security and Defence Policies of the Republic of Kosovo; to define the Strategic Security Environment, and possible security Risks and Threats; to analyse the current capacities of internal security institutions; to define the capacities that internal security institutions need in the future; to make recommendations for developing necessary capacities and the dissolution of those not needed, based on SSSR capabilities analysis; to provide guidance for new National Security Strategy of Kosovo; to provide recommendations for necessary legislative changes; and to establish security institutions based on SSSR recommendations and based on the National Security Strategy.

INTERNATIONAL ENVIRONMENT

Kosovo even though a small country is not immune to global trends, threats and risks. The international security environment has become unpredictable and challenging. Therefore, Kosovo is threatened by the phenomenon's such as economic inequity, trans-national crime, terrorism, proliferation of small arms, organized crime, trafficking of human begins and cyber-crime.

REGIONAL DYNAMICS

Kosovo considers that in 2014 the regional tensions, especially those between Kosovo and Serbia have open way for cooperation and partnership in the framework of the European integration, while NATO presence in the region remains a guarantee of security and stability. However, the region is still vulnerable to threats and risks such as ethnic and religious extremism, organized crime and trafficking off small arms and light weapons, etc.

INTERNAL THREATS

The SSSR has identified a number of conventional and non-conventional threats that endanger internally Kosovo. These threats are weak rule of law, corruption, organized crime, economic underdevelopment, unemployment, natural disasters, small arms, contested borders, unexploded explosives, cyber-crime and misuse of natural resources.

In order to address these threats the SSSR has made a set of recommendations. These recommendations include review of the legislation, development of the national security strategy, strengthening the emergency response capacities, drafting of the national defence strategy, review of the mandate of the assembly committees and establishment of a working group to start the process of preparation for NATO accession.

ANALYSIS: INTERNATIONAL VERSUS LOCAL DRIVEN SSR

Kosovo has only recently gained its independence, thus its experience in SSR is not comparable to most of the countries of the world. However, lack of experience cannot undermine its achievements; on the contrary Kosovo is a good example for SSR research and model for other countries, especially for post-conflict countries, to learn from the weaknesses and strengths of the Kosovo SSR.

Essentially Kosovo so far had only three SSR. The first SSR (1999) was basically a demilitarization process that transformed a military group KLA into an emergency, search and rescue civilian organization and establishment of a police force. This was a limited SSR, thus I will not deliberate further on this.

The ISSR was an extensive consultative process that included review of the security mechanisms in Kosovo, key governance institutions and, above all it, included citizens in the process to find out about their security concerns and threats. The methodology used in Kosovo as stated above is unique worldwide. While generally the SSR implies an endeavour intrinsic to security institutions, mainly including military, police and/or intelligence services, ISSR gives a central role to research threats and security concerns of the citizens. Such an approach has generated an immense amount of data that provided a comprehensive assessment for security threats of Kosovo.

"THE SSSR HAS IDENTIFIED A NUMBER OF **CONVENTIONAL AND NON-CONVENTIONAL** THREATS THAT ENDANGER INTERNALLY KOSOVO. **THESE THREATS ARE WEAK RULE OF LAW,** CORRUPTION, ORGANIZED CRIME, **ECONOMIC** UNDERDEVELOPMENT, UNEMPLOYMENT, **NATURAL DISASTERS, SMALL ARMS**, CONTESTED BORDERS, UNEXPLODED EXPLOSIVES, **CYBER-CRIME AND MISUSE OF NATURAL RESOURCES."**

The ISSR was an internationally driven process in cooperation with Kosovo local institutions. This fact contributed to overarching SSR in Kosovo which was extensive content and qualitative wise. It identified immediate and long term security threats to Kosovo, internal and external security risks, institutional gaps; and fears and concerns of the citizens. The recommendations of the ISSR have served for the security sector reform in post independent Kosovo and still even today help in shaping the Kosovo's security policy.

On the other hand, the SSSR was conducted under local ownership. The SSSR was comparatively far more limited in content and qualitative terms, than the ISSR. Even though the SSSR claims that the civil society has helped to shape and validate Kosovo's security concerns and threats, inclusion of the public was inadequate compared to ISSR. Moreover, the governance institutions research was shallow, whereas the main focus was given to the security institutions, particularly to the ministry of defence and Kosovo security forces. While it is understandable that Kosovo after its independence was striving to formally establish its armed forces under a civilian oversight, undermining other structural gaps and particularly the security concerns of the citizens' can produce other long term consequences. Therefore, the SSSR was basically a classical SSR having the main focus on security institutions, with superficial consideration towards threats that weak governance institutions can produce and the risks Kosovo citizens are exposed to such as poverty, unemployment, drugs, trafficking, extremism, etc.

CONCLUSIONS

This article has analysed the Kosovo's experience on SSR. As stated Kosovo's experience on SSR is only recent, however, it can provide a valuable knowledge on the methodology used and practices applied that can serve as lessons learned for other countries worldwide.

Aside of the 1999 demilitarization process, Kosovo had two different approaches in conducting the SSR in 2006 (ISSR) and 2014 (SSSR). While the ISSR was an international driven SSR in Kosovo that was a holistic process and included review and analysis of security and governance institutions, as well as fears and security threats of the citizens; the SSSR was locally driven process with the main focus on security institutions. The ISSR was more structured and comprehensive research that produces extensive data on security threats to Kosovo, the SSSR on the other hand was much more limited and was focused mainly on defence related issues.

Thus, it is safe to say that Kosovo's experience shows that locally driven SSR are more limited than those internationally driven, and that locally driven SSR focus on the immediate security sector concerns rather on the holistic states and citizens' security threats. While arguably it is justifiable, considering the sensitivity of the security matters that states have the right and exercise the authority to conduct the SSR, however, Kosovo's experience shows the valuable contribution of the external factor in this process. Therefore, I conclude that Kosovo's experience warrant for inclusion in the SSR process of the specialized organizations such as UN or EU or other organization in order to ensure comprehensive SSR that would identify security threats taking into consideration views of both state institutions and citizens; and provide inclusive and practical solutions on how to deter threats. This is crucial for understanding and applying comprehensive SSR since as stated in the analysis it is little worth of having a developed and efficient security sector if the population of the country is ill-educated, unemployed and unhealthy, vulnerable to drugs, trafficking, extremism, etc.

Fotografía:Ejército Nacional de Colombia

BIBLIOGRAFÍA

United Nations. (17 May 2019). *United Nations High Commissioner For Refugees Evaluation And Policy Analysis Unit The Kosovo refugee crisis. An independent evaluation of UNHCR's emergency preparedness and response*. Obtenido de https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/kos%20S2004%20932.pdf

United Nations. (2000). *The Kosovo refugee crisis. An independent evaluation of UNHCR's emergency preparedness and response.* Obtenido de https://www.unhcr.org/3ba0bbeb4.pdf

United Nations Security Council. (7 June 1999). *Letter dated 4 June 1999 from the permanent representative of France to the United Nations addressed to the Secretary General* . Obtenido de: https://peacemaker.un.org/sites/peacemaker.un.org/files/990123_RambouilletAccord.pdf

United Nations Security Council. (10 June 1999). *UNSC Resolution No. 1244.* Obtenido de: https://peacemaker.un.org/sites/peacemaker.un.org/files/990610_SCR1244%281999%29.pdf

UN Interim Administration Mission in Kosovo. (21 September 1999). *Kouchner signs regulation on Kosovo Protection Corps.* Obtenido de: https://reliefweb.int/report/serbia/kouchner-signs-regulation-kosovo-protection-corps

United Nations Security Council. (30 November 2004). *Letter dated 17 November 2004 from the Secretary-General addressed to the President of the Security Council.* Obtenido de: https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/kos%20S2004%20932.pdf,

ISSR. (2006). *Kosovo Internal Security Sector Review* . Obtenido de https://www.academia.edu/11057284/Kosovo_Internal_Security_Sector_Review

European Council. (1993). *Europan council in Copenhagen 21-22 June 1993. Conclusions of the presidency.* Obtenido de: https://www.consilium.europa.eu/media/21225/72921.pdf

United Nations Security Council. (26 March 2007). *Letter dated 26 March 2007 from the Secretary-General addressed to the President of the Security Council* . Obtenido de: https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/Kosovo%20S2007%20168.pdf

Republic of Kosovo. (2014). *Analysis of the strategic security sector review of the Republic of Kosovo.* Obtenido de: http://www.kryeministri-ks.net/repository/docs/Analysis_of_Strategic_Security_Sector_Review_of_RKS_060314.pdf

SECURITY SECTOR REFORM (SSR): THE TUNISIAN CONTEXT

Maxime L. Poulin

Maxime L. POULIN is the deputy head of office of DCAF in Tunisia where he spearheads the programmes with the Tunisian Ministry of National Defence and the Tunisian Parliament (l'Assemblée des Représentants du Peuple - ARP). Before joining DCAF, Maxime was a political and policy advisor with the Government of Canada, serving noticeably in the Cabinet of the Minister of Foreign Affairs and in the Cabinet of the Leader of the Official Opposition. He then joined the Washington based National Democratic Institute as a Senior International Field Advisor and, later, Rights & Democracy, a Montreal based organization, as Director of Development. Maxime has worked in advisory positions in the Democratic Republic of Congo, in the Republic of Guinea, and in Iraq. He holds a B.A. in History from the Université de Sherbrooke (Sherbrooke, Canada) and a M.A. in Public Communications from the Université Laval (Quebec City, Canada). He speaks French, English and conversational Spanish.

ABSTRACT

The article stated that Tunisia has made positive changes in terms of SSR while more work remains to be done in this area. Thus, an overview of the current security situation in Tunisia is made, providing a short theoretical background about the concept of SSR, in order to briefly describe some of the highlights of the SSR initiatives that were implemented in Tunisia since early 2011.

Palabras clave: *Security Sector Reform, democratic transition, human rights, policy-making*

REFORMA AL SECTOR SEGURIDAD: EL CONTEXTO TUNISIANO

RESUMEN

El artículo propone que Túnez ha realizado cambios positivos en términos de Reformas al Sector Seguridad (RSS), mientras que queda mucho trabajo por hacer en esta área. Por lo tanto, se hace una descripción general de la situación actual de la seguridad en Túnez, proporcionando una breve base teórica sobre el concepto de RSS, a fin de describir brevemente algunos de los aspectos más destacados de las iniciativas de RSS que se implementaron en Túnez desde principios de 2011.

Palabras claves: *Reforma al Sector Seguridad, transición democrática, derechos humanos, política pública*

INTRODUCCIÓN

Eight years ago, Tunisia experienced an unforeseen popular uprising that ended with the fall of Ben Ali's regime. The series of anti-government protests throughout the Arab world was sparked by the first protests that occurred in Tunisia, on December 18th, 2010, in Sidi Bouzid, following Mohamed Bouazizi's self-immolation in protest of police corruption and ill-treatment. In a way, this event set the table for a Security Sector Reform (SSR) Agenda, as it highlighted the link between the abuses and the impunity of a security sector apparatus and the fall of Ben Ali's regime. Since then, slowly and gradually, SSR is being implemented in Tunisia.

Theoretically, the democratic transition in Tunisia has given rise to a paradigm shift: security forces should now be service providers to Tunisian citizens and no longer be instruments used by the regime to remain in place. Within this new paradigm, and in order to restore confidence and establish trust between citizens and security forces, the government should aim at establishing an efficient, professional, accountable and affordable security apparatus. In this context, the SSR should aim to provide security institutions with the means and capabilities to ensure the security of citizens and the State. However, as it could be expected, there is a gap between theory and practice. This gap is perfectly understandable, as SSR is usually a slow process even in optimal situations.

In this article, we propose that Tunisia has made positive changes in terms of SSR while more work remains to be done in this area. We will start with an overview of the current security situation in Tunisia. Then, we will provide a short theoretical background about the concept of SSR. Only after that, we will attempt to briefly describe some of the highlights of the SSR initiatives that were implemented in Tunisia since early 2011.

CURRENT SECURITY SITUATION IN TUNISIA

Although the following account of the current security situation in Tunisia does not represent an exhaustive overview, it is worth highlighting the following elements:

- The current security situation is rather stable compared to previous years;
- Forces are better trained and probably more efficient now than after the fall of Ben Ali. This is particularly true when facing violent extremism;
- Intelligence coordination and national security mechanisms have improved in the last few years;

“Theoretically, the democratic transition in Tunisia has given rise to a paradigm shift: security forces should now be service providers to Tunisian citizens and no longer be instruments used by the regime to remain in place.”

> *SSR is the political and technical process of improving state and human security by making security provision, management and oversight more effective and more accountable, within a framework of democratic civilian control, the rule of law and respect for human rights.*

- Security forces regularly report successful operations aiming at dismantling terror cells;
- The border with Libya is protected by a buffer zone, with technical surveillance. It is also guarded by the military;
- With the cooperation of Algeria, Tunisia regained control of its western border.

Since 2011, Tunisia has enjoyed the most progressive and democratic legal framework for civil society in the Arab world. Broad protections for the exercise of freedom of association and support for a free and independent civil society sector are provided. Although the relations between civil society and authorities are not always harmonious, Tunisia's civil society has the capacity to provide crucial input to the SSR process. The extent to which this input is taken into account remains limited, but channels of communication do exist.

On a less positive note, there have been recurrent allegations of human rights violations by internal security forces since 2011. It is also worth noting that current citizen's support for security forces in the fight against terrorism does not constitute a lasting reconciliation of the citizens with the security forces, particularly with internal security forces.

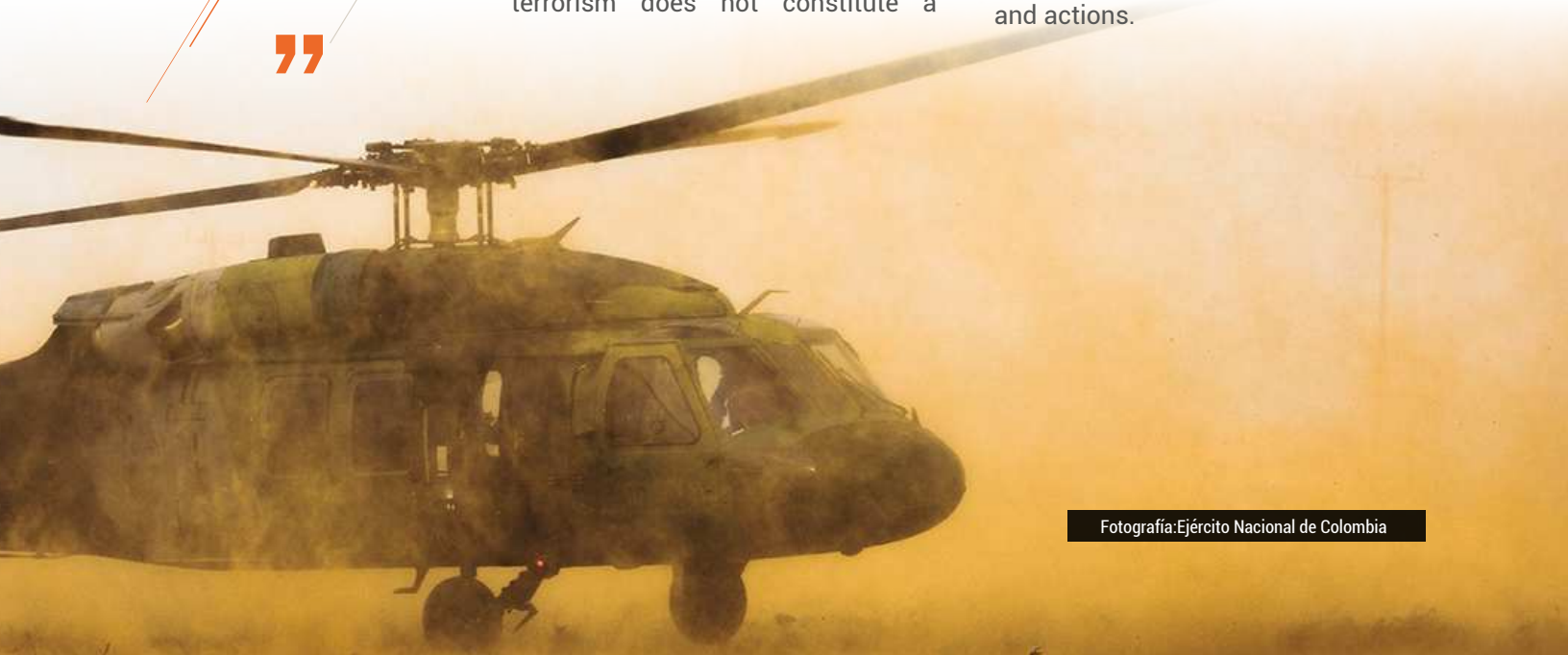
Besides, important smuggling activities have been taking place at the borders with Libya and Algeria.

Finally, improved and sustainable security cannot be achieved, in the long run, unless more support is provided to the Tunisian youth who suffer from all forms of socio-economic problems including poverty, unemployment and lack of economic opportunities.

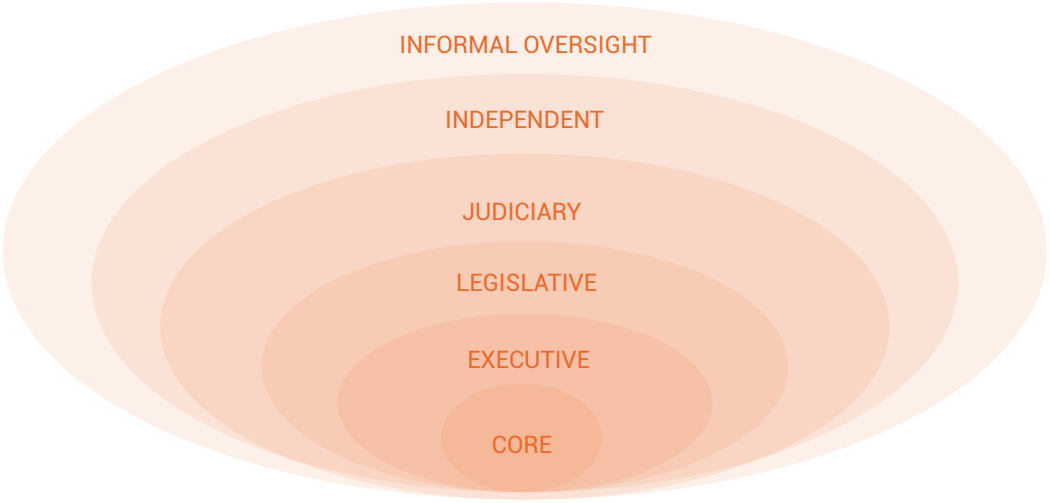
WHAT IS SSR?

SSR is the political and technical process of improving state and human security by making security provision, management and oversight more effective and more accountable, within a framework of democratic civilian control, the rule of law and respect for human rights.

The goal of SSR is to apply the principles of good governance to the security sector. SSR concerns all state and non-state actors involved in security provision, management and oversight, and emphasizes the links between their roles, responsibilities and actions.



Fotografía:Ejército Nacional de Colombia



Within the spirit of interdependence between security and justice, it is essential to highlight that SSR also involves aspects of justice provision, management and oversight. For instance, a more efficient justice system may gradually solve the issue of overcrowded prisons. SSR can include a wide range of different reform activities covering all political and technical aspects of security, including, among others, legislative initiatives; policy-making; awareness-raising and public information campaigns; management and administrative capacity building; infrastructure development; and improved training and equipment.

SSR EFFORTS IN TUNISIA

Legal Framework

Between 1956 and 2011, around 1700 legislative texts, of which 1200 are still in force, have been passed and adopted by the different Tunisian governments. A large number of these texts were enacted in the form of presidential decrees in order to legally manipulate the armed forces and coerce them to protect the regime instead of the people.

Since the events of 2010-11, a new legal framework has been gradually put in place. For example, the interim government of 2011 ratified the optional protocol to the Convention against Torture (and Other Cruel, Inhuman, or Degrading Treatment or Punishment), the International Convention for the Protection of All Persons from Enforced Disappearance and the Rome Statute of the International Criminal Court.

The 2014 Constitution guarantees rights and the rule of law. Tunisia has seen the ratification of several international instruments which relates to the work of the security sector. Important laws have been passed:

- The Law on access to information;
- The Law on the elimination of violence against women, and;
- The Law on the fight against corruption (which includes whistleblower protection and declaration of assets).

It is also worth noticing that a reform of Penal Code/ Penal Procedural Code is on its way.

However, these significant improvements are somehow impaired by the fact that the security sector does not appropriately meet the requirements of the new Constitution to this day. Its implementation is often complicated and the independence of the judicial reform process, which is an integral part of the SSR, is subject to political pressure.

Despite these promising steps, the regulations adopted by the new Constitution failed to provide clear and effective guidelines for the security sector. The Tunisian Constitution, being adopted in 2014, refers to the security forces only in one single article. Members of the National Constitutional

Assembly missed a great opportunity, during the phase of drafting the Constitution, to learn from other successful democratic transitions that implemented a system of checks and balances and effectively reformed their security apparatuses. The implementation of effective security sector reforms requires the ability to carefully examine international norms and standards and implement them in a way that they go in line with the context of the country. Unfortunately, this was not the case in Tunisia when drafting the 2014 Constitution.

THE POLICE REFORM PROCESS IN TUNISIA

The internal security forces administered by the Ministry of Interior (MOI) consist of the Police, the National Guard, the Judicial police, the presidential guard forces and the intervention forces. While the Police operates mostly in urban areas, the National Guard operates in other parts of the country. The Judicial police operates in the ministry of Justice (MOJ) but is administered by the Ministry of Interior. They are the investigative branch of the internal security officers and are responsible for collecting evidence and conducting investigations.

Since the fall of Ben Ali's regime, reforming the MOI has been one of the priorities of the various governments in Tunisia. The first promising sign of serious reform of Tunisia's security sector was

"THE **IMPLEMENTATION OF EFFECTIVE SECURITY SECTOR REFORMS** REQUIRES THE ABILITY TO CAREFULLY **EXAMINE INTERNATIONAL NORMS AND STANDARDS** AND IMPLEMENT THEM IN A WAY THAT THEY GO IN LINE WITH THE **CONTEXT OF THE COUNTRY. UNFORTUNATELY**, THIS WAS NOT THE CASE IN TUNISIA WHEN **DRAFTING THE 2014 CONSTITUTION**."

a white paper entitled "security and development: a white paper for democratic security in Tunisia", published by the Ministry of Interior in 2011, which included a comprehensive plan for reform. Besides, a human rights guide for the police was developed by the MOI and UNHCR. In 2011, the MOI also cooperated with the Geneva Centre for the Democratic Control of Armed Forces to conduct a preliminary study of the Ministry's communication approach with the public.

Notwithstanding great achievements, human rights violations and corruption persist, with less frequency, combined with weak parliamentary and independent oversight. Limited access to information remains the norm. All in all, oversight and accountability of the security sector remain a challenge as does the development of planning capabilities.

Since 2015, Tunisia succeeded in overcoming its fragile security situation and implementing positive steps forward. However, authorities' efforts were often hindered by the different social, economic and security needs. Due to the consensual nature of Government, ministries find it difficult to implement work plans agreed within the Government and/or international donors. Key security institutions are absorbed by managing the security situation and the steady inflow of bilateral security assistance (train & equip) leaving little room for further-reaching reforms.

SECURITY SECTOR REFORMS AND THE MINISTRY OF DEFENSE

Marginalized and confined to their barracks under Ben Ali's regime, the Tunisian military regained support from decision-makers. They also enjoy a lot of trust from the public at large. The Ministry of Defense's budget has significantly increased. The military also enjoyed a stream of weapons and equipment through international partnerships. For an external eye, it is easy to perceive that there is a lot of soul searching happening among the military ranks as to whether or not the institution should engage in more civilian outreach.

The previous regime had enabled Ben Ali to have total control over the military, given that the previous Constitution granted the President exclusive responsibility for military matters. However, after the fall of the country's strong man, the Constitution of 2014 reformed the high-level management of the military. Under this Constitution, the President of the Republic is responsible for appointing the top military positions in consultation with the President of the Government (Prime Minister). The President of the Republic is also responsible for declaring a state of emergency, setting the general state policies such

Fotografía:Ejército Nacional de Colombia

as white papers and leading the National Security Council. Meanwhile, the President of the Government is responsible for the supervision and the organization of the ministry of Defense. While this division of power is important and susceptible to prevent abuses, its application is ambiguous and subject to political influences.

In terms of access to information, the Ministry of Defense has embraced good practices in line with robust access to information laws. For instance, it was among the first ministries to send their annual reports on access to information. The Ministry also publishes the contact information of responsible officers of access to information as well as the different procedures. In 2017, the Ministry of Defense received 22 requests and provided responses to all of them within the 20-day limit imposed by the law. However, the issue lies with the content of the responses. The MOD often uses the national security argument as an excuse to avoid providing detailed answers to these requests. As it is the case for many official websites, the Ministry of Defense's website lacks relevant information, including procurement procedures, military and non-military acquisitions, auditing reports and statistics.

Nevertheless, there has been progress in terms of military-civil society relations. Indeed, many retired officers have become more active in educating the public and politicians about the military and have taken a proactive approach in providing the armed forces with guidance to help them meet their needs and advance their interests. As a result, several civil society organizations have been founded by retired officers, such as the Association of Former Officers of the National Army, the Tunisian Centre for Global Security Studies and the Association of Veterans of the National Defense Institute. These organizations are playing an active role in advancing a public debate over the armed forces by instigating proposals and providing recommendations.

"THERE HAS BEEN PROGRESS IN **TERMS OF MILITARY-CIVIL SOCIETY RELATIONS**. INDEED, MANY RETIRED OFFICERS HAVE BECOME MORE ACTIVE IN EDUCATING THE PUBLIC AND POLITICIANS ABOUT **THE MILITARY AND HAVE TAKEN A PROACTIVE APPROACH** IN PROVIDING THE ARMED FORCES WITH GUIDANCE **TO HELP THEM MEET THEIR NEEDS** AND ADVANCE THEIR INTERESTS."

Fotografía:Ejército Nacional de Colombia

CONCLUSION

It is fair to highlight that reforms implemented in Tunisia should be congratulated but relatively hindered by a lack of political will to go further and the affirmation, after the adoption of the 2014 Constitution, of a culture of resistance to change. As mentioned in one of DCAF's publications (2012): "one of the most challenging issues when engaging in SSR is to ensure that all stakeholders share the same objectives. This is particularly challenging, given the multiplicity of actors involved and because SSR touches on politically sensitive issues that often create winners and losers".

However, highlighting these challenges, as we just did, in no way represents a negative assessment of the Tunisian authorities' efforts to reform the security sector. Better results may be achieved through better planning capacities, better coordination between security services, and more strategic communication about the security sector reform process. Combined with long term engagement of international partners supporting better governance and human rights promotion activities, rather than mostly ensuring short terms security arrangements, the security sector reform process in Tunisia could potentially live up to the expectations that emerged in the aftermath of the Tunisian revolution of January 2011.

"COMBINED WITH LONG TERM ENGAGEMENT **OF INTERNATIONAL PARTNERS** SUPPORTING BETTER GOVERNANCE AND **HUMAN RIGHTS PROMOTION ACTIVITIES,** RATHER THAN MOSTLY ENSURING SHORT TERMS SECURITY ARRANGEMENTS, **THE SECURITY SECTOR REFORM PROCESS IN TUNISIA** COULD POTENTIALLY LIVE UP TO THE EXPECTATIONS **THAT EMERGED IN THE AFTERMATH** OF THE TUNISIAN REVOLUTION OF JANUARY 2011."

BIBLIOGRAFÍA

Hicri, S., & Tlili, K. (2018). A study on youth perception of human security at the local level. DCAF Tunisie.

DCAF. (2012). *SSR in a nutshell: Manual for introductory training on Security Sector Reform*. Geneva: DCAF.

UNA REFORMA AL SECTOR DE SEGURIDAD (RSS)CON PERSPECTIVA DE GÉNERO - UN REQUISITO ESENCIAL PARA UN SECTOR DE SEGURIDAD REPRESENTATIVO Y SOSTENIBLE.

Martin Åhlin

Especialista Mujeres, Paz y Seguridad, Departamento de Operaciones de Paz, Liderazgo y Genero, Folke Bernadotte Academy (FBA). Con contribuciones de Anna Johansson, Asesora Mujeres, Paz y Seguridad, FBA y Marcelo Díaz, Agregado de Cooperación para Paz y Seguridad Embajada de Suecia en Colombia.

Jenny Lindqvist

Asesora de RSS, Departamento de Prevención de conflicto, Consolidación de Paz y Gobernanza

La Academia Folke Bernadotte (FBA) es la agencia gubernamental sueca para la paz, la seguridad y el desarrollo en países afectados por conflictos armados. En Colombia, por mandato del gobierno sueco, la FBA está apoyando los esfuerzos en la construcción de la paz sostenible de actores estatales y de la sociedad civil.

RESUMEN

La integración de una perspectiva de género es ampliamente reconocida como uno de los principios clave de la Reforma del Sector de Seguridad (RSS). Sin embargo, a pesar de esto, la perspectiva de género, en muchos casos, no es abordada estratégicamente en la planificación y la implementación práctica de la RSS. Muchas veces la perspectiva ni siquiera es considerada. La falta de considerar una perspectiva de género en la RSS impide que el proceso de reforma contribuya a un sector de seguridad eficaz, responsable y sostenible. Los factores que contribuyen a esta oportunidad perdida son, a menudo, malentendidos, relacionados con el concepto de género en sí mismo, por ejemplo, frente a que los aspectos de género solo afectan a las mujeres o que se puede agregar una perspectiva de género después de ya haberse diseñado el proceso de reforma. De hecho, la integración de una perspectiva de género es un componente fundamental de la RSS, por lo que debe integrarse de manera adecuada y estratégica en todo el proceso de reforma.

Palabras clave: *RSS, género, seguridad humana, perspectiva de género.*

ABSTRACT

The integration of a gender perspective is widely recognized as one of the key principles of security sector reform (SSR). However, despite this, the gender perspective, in many cases, is not addressed strategically in the planning and practical implementation of RSS. Many times, the perspective is not even considered. The failure to consider a gender perspective in the RSS prevents the reform process from contributing to an effective, responsible and sustainable security sector. Factors that become a lost opportunity are often misunderstood, related to the concept of gender in itself, for example, that gender aspects only affect women and that a gender perspective can be added after being designed the reform process. In fact, the integration of a gender perspective is a fundamental component of the SSR, which must be integrated appropriately and strategically throughout the reform process.

Keywords: *SSR, gender, human security, gender perspective.*

Fotografía:Ejército Nacional de Colombia

LA SEGURIDAD HUMANA – ¿LA SEGURIDAD DE QUIÉN?

El concepto de la RSS se funda en la seguridad humana. Esto significa que la RSS tiene un enfoque de seguridad centrado a las personas, basado en la seguridad de cada individuo. Esto no significa que los conceptos tradicionales de seguridad, relacionados con, por ejemplo, la protección del territorio y la soberanía del Estado, carezcan de importancia. La entrega de la seguridad humana y estatal debe considerarse más bien como un refuerzo mutuo, pero un enfoque de seguridad humana garantiza que las inseguridades de los individuos, mujeres y hombres, estén en el centro del análisis, lo que hace que la inclusión de una perspectiva de género en la entrega de la RSS sea un componente fundamental

EL MARCO NORMATIVO DE LA PERSPECTIVA DE GÉNERO Y RSS

15 años han pasado desde que el Consejo de Seguridad de las Naciones Unidas adoptó su primera resolución sobre mujeres, paz y seguridad, la reconocida RCSNU 1325. Una resolución innovadora ya que llevó la situación de las mujeres y las niñas en situaciones de conflicto y posconflicto al núcleo de la gestión internacional de la paz y la seguridad: el Consejo de Seguridad de la Organización de las Naciones Unidas. La previa falta de priorización de las necesidades particulares de las mujeres y las niñas en situaciones de conflicto y posconflicto finalmente recibió una atención muy necesaria. La RCSNU 1325 fue seguida por ocho resoluciones más, que ampliaron los temas referidos en la primera resolución. Juntas, estas nueve resoluciones forman la Agenda sobre mujeres, paz y seguridad. Una agenda cada vez más amplia y relevante, ya que la última resolución 2467 fue adoptada el 23 de abril de este año.

Fotografía: Ejército Nacional de Colombia

[1] Hay varias otras formas de resumir su contenido. La prevención y la asistencia son temas que se mencionan a menudo, pero la participación, la protección y la Transversalicación del Enfoque de Género (TEG) también lo abarcan e incluyen

[2] UN Security Council, Report of the Secretary-General on securing states and societies; strengthening the United Nations comprehensive support to security sector reform, 13 August 2018, S/2013/480.

[3] UN Security Council, Security Council resolution 2151 (2014) on security sector reform) 28 April 2014, S/RES/2151 (2014).

Desde su inicio, la agenda de mujeres, paz y seguridad ha progresado continuamente y muchas instituciones regionales y nacionales han desarrollado marcos de políticas generales que reconocen el contenido de la agenda cuyo contenido se puede sumar en tres pistas: la necesidad de integrar una perspectiva de género, promover la participación y robustecer la protección de la mujer en el contexto de la construcción de la paz[1]. Los mismos temas se repiten y enfatizan también en el marco político colombiano para la igualdad de género, entre otros, la Política Pública Sectorial de Transversalización del enfoque de Género para el Personal Uniformado de La Fuerza Pública. El mismo enfoque también está presente en el marco internacional para la RSS, como el informe de 2013 del Secretario General de la ONU sobre la RSS que también recalca la importancia de vincular las actividades de la RSS al análisis de género[2]. De manera similar, la primera Resolución del Consejo de Seguridad de la ONU sobre RSS, RCSNU 2151, adoptada en 2014, enfatiza la importancia de la participación equitativa efectiva y plena de la mujer en la RSS[3].

La Reforma del Sector de Seguridad (RSS) es un componente fundamental en la cooperación internacional para el desarrollo, el cual está orientado a la creación de un entorno seguro para la población, así como posibilitar que las instituciones de seguridad asuman papeles eficaces, legítimos y democráticamente responsables en el cumplimiento de su misionalidad, asegurando la paz, democracia y desarrollo socioeconómico sustentable. La Organización para la Cooperación y el Desarrollo Económicos- OCDE- avaló en el año 2004, los objetivos y principios rectores para una reforma estructural del Sector Seguridad (OCDE/DAC Handbook 2008) con especial énfasis en los retos y desafíos que implica este proceso.

“La Reforma del Sector de Seguridad (RSS) es un componente fundamental en la cooperación internacional para el desarrollo, el cual está orientado a la creación de un entorno seguro para la población, así como posibilitar que las instituciones de seguridad asuman papeles eficaces, legítimos y democráticamente responsables en el cumplimiento de su misionalidad, asegurando la paz, democracia y desarrollo socioeconómico sustentable. La Organización para la Cooperación y el Desarrollo Económicos- OCDE- avaló en el año 2004, los objetivos y principios rectores para una reforma estructural del Sector Seguridad (OCDE/DAC Handbook 2008) con especial énfasis en los retos y desafíos que implica este proceso.”

Fotografía: Escuela de suboficiales (EMSUB) Ejército Nacional de Colombia

Fotografía:Ejército Nacional de Colombia

"EN EL GLOSARIO DE LA **POLITICA PÚBLICA SECTORIAL** DE TRANSVERSALIZACIÓN DEL ENFOQUE DE GÉNERO **PARA EL PERSONAL UNIFORMADO** DE LA FUERZA PÚBLICA SE EXPLIQUE LO QUE SIGNIFICA **"GÉNERO"**"

DIFERENTES NECESIDADES DE SEGURIDAD

Analizar las diferentes necesidades de seguridad de las mujeres/los hombres/ los niños/las niñas respectivamente, lo que se llama hacer un análisis de género, es una forma muy concreta y directa de aplicar una perspectiva de género a una situación de seguridad. ¿Cuáles son las diferentes necesidades de seguridad de los diferentes grupos? Debería ser una de las primeras preguntas que tendría hacer una misión/operación nacional o internacional cuyo mandato es mejorar la seguridad de la población de un país/ área. Todas las mujeres no tienen las mismas necesidades de seguridad (por el mero hecho de que sean mujeres) y todos los hombres no tienen las mismas necesidades de seguridad (por el mero hecho de que sean hombres). Aspectos como la etnia, la economía, la orientación sexual o identidad de género, la religión, dónde vive o de dónde proviene una persona (zona rural/urbana) y la cultura, también determinan las necesidades de seguridad de las personas, lo que se llama: el enfoque diferencial. Los hombres/las mujeres/las niñas/los niños también tienen necesidades de seguridad comunes. No obstante, identificar las diferencias garantiza que no se pase por alto ninguna necesidad de seguridad.

En el glosario de la Politica Pública Sectorial de Transversalización del Enfoque de Género para el Personal Uniformado de la Fuerza Pública se explique lo que significa "Género":

"El género se refiere a las normas que una sociedad construye para definir 'qué es y cómo deben ser las mujeres' y, así mismo, 'qué es y cómo deben ser los hombres', en términos de sus identidades, características, roles, orientaciones sexuales y comportamientos. Sin embargo, históricamente, las relaciones

de género se han construido a partir de relaciones de poder que han privilegiado lo masculino sobre lo femenino, dando al primero una posición de poder y dominio mientras lo femenino ocupa una posición de desventaja y subordinación en la sociedad, así como se han generado formas de opresión y discriminación hacia personas que no se acomodan a las expectativas sociales del 'ser hombre y 'ser mujer'." (Ministerio de Defensa, 2018).

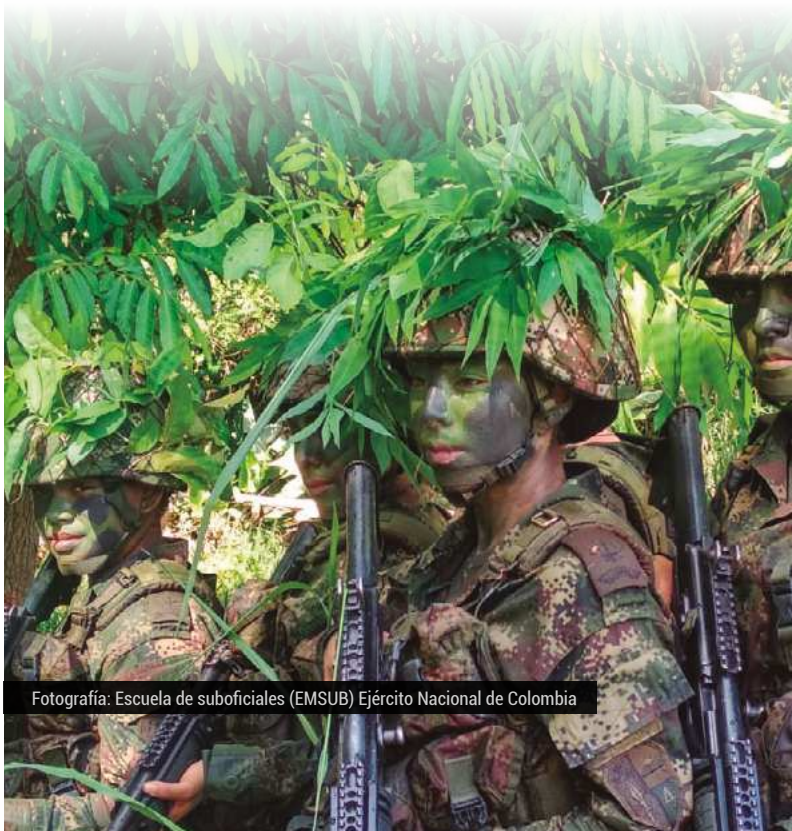
¿Por qué integrar una perspectiva de género en la Reforma del sector de la seguridad?

Los roles de género predominantes en muchos de los contextos sometiéndose RSS sigue previniendo la participación equitativa y significativa de mujeres y hombres en los procesos de reforma. En muchos contextos, los roles de género predominantes conducen a que menos mujeres sean admitidas a, o quieran ser parte, del sector de seguridad. Debido a que las mujeres tienden a estar en minoría en el sector de la seguridad, un enfoque sensible al género a menudo incluye estrategias para promover y aumentar la participación de las mujeres en el sector. Sin embargo, esto a veces contribuye a la idea errónea de que incluir una perspectiva de género solo concierne a la participación de las mujeres. Muy por el contrario; igualmente importante es para la RSS sensible al género comprender las normas de masculinidad y cómo éstas pueden contribuir a inseguridades específicas para hombres y niños.

> "El papel de los hombres como proveedores es una norma universal y el trabajo es fundamental para comprender como el hecho de estar desempleado, los bajos ingresos o la falta de estatus en el lugar de trabajo pueden fomentar una baja autoestima y una sensación de fracaso como proveedor. Los sentimientos de insuficiencia pueden llevar a los hombres y niños a recurrir al abuso de sustancias, a migrar, a la depresión y a conductas sexuales peligrosas. La Violencia, incluso dirigida a si mismo, puede convertirse en una demostración o reafirmación del poder masculino para restablecer su estatus en la sociedad." (Barker, G., Contreras, J.M., et al., 2014)

Comprender por qué el género es importante para la RSS requiere una comprensión tanto del concepto de RSS como del concepto de género. Por ejemplo, en la posibilidad de considerar el impacto directo en la división del trabajo entre hombres y mujeres y sus respectivas posibilidades de acceder y controlar los recursos y el poder. Una cosa es poder lograr acceder a recursos, cualquiera que estos sean, y otra distinta es tener pleno control sobre los mismos recursos.

Las **nociones de feminidad y masculinidad** también interactúan con otros aspectos de la identidad que influyen en el poder, como la edad, el origen étnico y la clase social, por nombrar algunos. La RSS sensible al género requiere una comprensión de cómo todos estos aspectos interactúan y producen diferentes formas de desigualdades en relación, por ejemplo, con la protección contra la violencia, el acceso a servicios de seguridad y las oportunidades para influir en las prioridades de seguridad. El objetivo de la RSS es consolidar un sector de seguridad democrático, representativo y sostenible que se adhiera a los principios de derechos humanos y al estado de derecho. La RSS se esfuerza por contribuir a un sector de seguridad que sea capaz y también responsable de brindar seguridad a su población. Esto implica un proceso de reforma inclusivo que toma en consideración los diferentes roles de género aplicados a hombres, mujeres, niños y niñas en cada contexto. Es un proceso de reforma que promueve la igualdad de género asegurando que las necesidades de seguridad, las experiencias y las perspectivas de todas las partes de la población son reconocidas y respetadas por igual cuando se planifica y aplica la RSS.



Fotografía: Escuela de suboficiales (EMSUB) Ejército Nacional de Colombia

¿Cómo se puede implementar una RSS sensible al género?

La integración de una perspectiva de género en la RSS es una estrategia para garantizar que las preocupaciones y experiencias de hombres y mujeres, niños y niñas formen parte integral del diseño, la implementación, el monitoreo y la evaluación de la RSS. Es un método para promover la igualdad de género y asegurar que la desigualdad no se perpetúe por ninguna actividad del proceso de reforma. Para lograr una RSS sensible al género es necesario crear un sector de seguridad y una arquitectura organizativa representativa y confiable para una incorporación efectiva de la perspectiva de género.

HERRAMIENTAS PARA UNA RSS SENSIBLE AL GÉNERO

Transversalización del enfoque de género (TEG)

Para integrar eficientemente una perspectiva de género, se le debe dar prioridad, y se debe crear una arquitectura nacional y organizativa para la transversalización del enfoque de género. A nivel nacional, esto significa el desarrollo de una legislación que promueva y exija la igualdad de derechos para hombres y mujeres y la creación de mecanismos de supervisión, como una oficina ministerial y un ministro para la igualdad de género, que puedan apoyar y coordinar a las agencias gubernamentales en su trabajo por la igualdad de género, por nombrar solo dos medidas cruciales. En el nivel organizativo, esto significa la creación de políticas internas con respecto a la transversalización del enfoque de género, que pueden guiar la implementación de la perspectiva de género y los esfuerzos para aumentar el equilibrio de género dentro de la organización.

El compromiso del más alto liderazgo, así como de la gerencia media, es clave para transversalizar el enfoque de género de manera efectiva. Ellos tienen una clara responsabilidad de implementación que debe destacarse en las políticas internas. Para respaldar y asesorar la implementación y el uso continuo del análisis de género, se deben crear unidades de género o posiciones expertas en género. Otro ejemplo de una medida efectiva es la estandarización y la realización rutinaria de iniciativas de capacitación para el liderazgo, así como para todo el personal en la integración de la perspectiva de género, algo que la unidad de género o el asesor podrían ser responsables de desarrollar. Implementar tales medidas es crucial para los proveedores de seguridad, ya que les permitirá cumplir sus obligaciones para todas las partes de la población.

El núcleo de la integración de la perspectiva de género es la evaluación constante de las consecuencias que pueda tener cualquier acción para hombres y mujeres, y luego la adaptación de las actividades para evitar la discriminación. Con una arquitectura de género que funcione bien dentro de una organización, este será un objetivo alcanzable.

En palabras del ex Director General de la Policía Nacional, General Jorge Hernando Nieto Rojas, "incorporar la perspectiva de género/TEG en la Policía Nacional significa, en primera instancia, reconocer la existencia social y cultural de relaciones desiguales en donde las mujeres son subordinadas y sometidas a múltiples formas de discriminación y violencia"[4]

Transversalización del enfoque de género es "el proceso de evaluación de las consecuencias para las mujeres y los hombres de cualquier actividad planificada, incluyendo leyes, políticas

[4] Palabras del Director General Policía Nacional, General Jorge Hernando Nieto Rojas, en el lanzamiento del Proyecto Ema de la Policía Nacional-UNIPEP en Bogotá DC el 6 de julio de 2018. EMA equivale a Equipos Móviles de Atención, nombre operativo que se le dio al proyecto de la Policía Nacional para la incorporación del Enfoque de Género en el Servicio de Policía. Este proyecto piloto, busca prevenir y atender las violencias basadas en génenero en 7 municipios del país particularmente afectados por este tipo de violencias.

o programas, en todos los sectores y a todos los niveles. Es una estrategia destinada a hacer que las preocupaciones y experiencias de las mujeres, así como las de los hombres, sean un elemento integral de la elaboración, la aplicación, la supervisión y la evaluación de las políticas y los programas en todas las esferas políticas, económicas y sociales, a fin de que las mujeres y los hombres se beneficien por igual y se impida que se perpetúe la desigualdad. El objetivo final es lograr la igualdad entre los géneros." (UNECOSOC, 1997)

ANÁLISIS DE GÉNERO

El análisis de género debe realizarse de manera consistente desde el inicio de cualquier actividad planificada, y debe ser actualizado a lo largo de la implementación de la actividad. Como se mencionó en la introducción, no será efectivo si se agrega como una idea de último momento al final de la planificación.

Realizar un análisis de género significa hacer preguntas adicionales al planificar, realizar o evaluar tareas o iniciativas. Ampliando el Modelo de Harvard[5], las preguntas que utiliza la FBA en su modelo de análisis de género se dividen en cinco perfiles diferentes:

Perfil de representación y actividad – Este perfil se refiere a la división por género de los roles y responsabilidades preguntando ¿quién hace qué, dónde y cuándo? ¿Qué hacen las mujeres, los hombres, los niños, las niñas? ¿Dónde están?

Perfil de recursos - A través de sus roles y responsabilidades, hombres y mujeres, niños y niñas, tienen diferente acceso a los recursos, y control de los mismos. En este perfil, hacemos preguntas sobre quién tiene el acceso y control de qué recursos.

Perfil de actitudes sociales - Las actitudes sociales (estereotipos, expectativas) afectan de diferente manera a las mujeres y a los hombres, y las niñas y niños, por lo que hacemos preguntas sobre quién se ve afectado por qué actitudes sociales.

Perfil de protección/ inseguridades - Este perfil analiza las posibles diferentes inseguridades/necesidades de protección/preocupaciones entre mujeres, hombres, niños y niñas. ¿Quién enfrenta qué tipo de inseguridades/ necesidades de protección?

Perfil de consecuencias/ impacto - Aquí es donde preguntamos cuáles son las consecuencias o cuál es el impacto de los perfiles anteriores sobre las mujeres, los hombres, las niñas y los niños. La respuesta nos informa cuáles son las necesidades, intereses y oportunidades específicas de género.

Si una organización que trabaja con seguridad convierte en habitual hacerse esas preguntas, respondérselas y adaptar sus acciones para que las desigualdades descubiertas mediante el análisis fuesen remediadas, progresarían mucho en cumplir su compromiso con respecto a la igualdad de género, y sin duda serían un proveedor de seguridad más efectivo.

[5] El marco de Harvard se describe originalmente en Overholt, Anderson, Cloud and Austin, Gender Roles in Development Projects: A Case Book, 1984, Kumarian Press: Connecticut.

Fotografía:Ejército Nacional de Colombia

EQUILIBRIO DE GÉNERO

Un sector de seguridad con equilibrio de género significa tener la representación equitativa de mujeres y hombres en todas las áreas de trabajo y en todos los niveles, incluso en cargos directivos. La igualdad de oportunidades entre hombres y mujeres es un derecho humano fundamental y se destaca en numerosos compromisos y convenciones internacionales[6]. Las agencias y entidades gubernamentales encargadas de brindar seguridad a la población, deben ser representativas de la población y reflejar su composición y, en muchos casos, contar con personal masculino y femenino es una necesidad operativa (Valasek, 2008). También se sabe que un sector de seguridad con mayor equilibrio de género es más eficaz, dado que, entre otros, permite maximizar los recursos y capacidades de cada uno de sus miembros independiente de su sexo, orientación sexual o identidad de género[7]. Sin embargo, el apoyo a una fuerza laboral más equilibrada en materia de género, especialmente dentro de las funciones básicas de seguridad, a veces se construye de una manera que refuerza los rígidos roles de género en lugar de centrarse en crear un sector de seguridad inclusivo y más democrático donde hombres y mujeres ocupen todos los cargos en todos los niveles.

CONCLUSIÓN

Un sector de seguridad con perspectiva de género- representación, eficiencia y sostenibilidad

Trabajar con una perspectiva de género beneficia a todos. Lo hacemos porque es correcto, pero también porque es útil y favorable para nuestro trabajo. Una perspectiva de género amplía nuestra perspectiva, nos ayuda a establecer procesos más inclusivos y lograr resultados más sostenibles. Por lo tanto, es imprescindible para todos los esfuerzos de construcción de la paz.

Como lo reconocen numerosos acuerdos y estrategias internacionales, la igualdad de género es una parte esencial de una sociedad pacífica y democrática. La RSS, cuyo objetivo es garantizar la provisión de seguridad humana para todas las partes de la población, tiene la responsabilidad específica de ser sensible al género. La RSS sensible al género también es un requisito previo para una reforma exitosa, ya que influirá y se verá afectada por las dinámicas de poder desafiadas. Para fortalecer la RSS sensible al género en la práctica, sin embargo, es necesario alejarse de la comprensión simplista e inexacta de qué es el género y cómo se relaciona con la RSS. Es imperativo fortalecer la integración de una perspectiva de género en todas las etapas de la RSS, desde el análisis inicial y la implementación, hasta el monitoreo y la evaluación de la reforma.

De acuerdo con esto, las herramientas para una reforma del sector de la seguridad con perspectiva de género, deben ser parte integral de cualquier iniciativa de RSS. Un proceso de RSS sensible al género contribuye a crear las bases para una sociedad más pacífica y democrática.

LA ACADEMIA FOLKE BERNADOTTE (FBA) APOYA LOS ESFUERZOS DE CONSTRUCCIÓN DE LA PAZ EN COLOMBIA

La Academia Folke Bernadotte (FBA) es la agencia gubernamental de Suecia dedicada a asuntos relacionados con la paz, la seguridad y el desarrollo. La FBA ejerce su mandato en el área de operaciones de paz, y de misiones de cooperación a nivel internacional. La agencia está dedicada a construir

[6] Ver por ejemplo: The Universal Declaration of Human Rights and the Convention on the Elimination on All Discrimination against Women (CEDAW).

[7] Ver por ejemplo: Gender Equality and Security Sector Reform, mainstreaming gender equality in security provision, management and oversight. SSR Backgrounder, Geneva Centre for the Democratic Control of Armed Forces.

procesos de capacitación y formación, y a investigar y desarrollar metodologías para apoyar esfuerzos en materia de construcción de paz y fortalecimiento del Estado en países en situación de conflicto o posconflicto. De igual manera, la FBA contrata y despliega personal civil para operaciones de paz y misiones de observación electoral dirigidos por la UE, la ONU y la OSCE. La agencia lleva el nombre del primer mediador de la ONU, Folke Bernadotte

Dentro del marco de la estrategia de cooperación bilateral con Colombia 2016-2020, la FBA se enfoca principalmente en tres areas temáticas;

Transformación/Reforma del Sector de Seguridad (TSS/RSS): La FBA dirige sus esfuerzos en temas de RSS a individuos y entidades relevantes dentro del Ministerio de Defensa y la Fuerza Pública igual que representantes del Congreso y sociedad civil, organizando cursos de formación y eventos de intercambio de experiencias con investigadores academicos para aumentar el nivel de conocimiento de aspectos importantes como la gobernanza del sector de seguridad. En 2018 se organizó por primera vez un curso de RSS en español en Colombia (igual que en los otros areas temáticos), dirigido a representantes de la Fuerza Pública (las tres Fuerzas, la Policía , el Ministerio de Defensa, el Comando de Transformación Ejército del Futuro - COTEF, etc.) El enfoque principal del curso era de aumentar los conocimientos del marco internacional normativo de la RSS y entender los objetivos, principios y procesos de la RSS.

Desarme, Desmovilización y Reincorporación (DDR): FBA brinda apoyo a entidades de la Fuerza Pública que desempeñan un papel en temas de desarme y desmovilización, y ofrece actividades de capacitación. También colabora con la ARN (Agencia para la Reincorporación y Normalización) en su trabajo de reincorporación de los excombatientes de las FARC. La colaboración consiste en capacitación en modelos de reincorporación y construcción de paz territorial. Así, la FBA desde hace varios años ha sido, y sigue siendo un socio para la organización de foros regionales en zonas afectadas por el conflicto armado.

Mujeres, Paz y Seguridad: Con fundamento en la Resolución 1325 del Consejo de Seguridad de la ONU, y otras resoluciones sucesivas, FBA respalda entidades del Estado Colombiano (la Fuerza Pública y ARN, entre otros) en la integración de una perspectiva de género en sus organizaciones y su misionalidad. Actividades de capacitación basadas en la pedagogía desarrollada por FBA, asesoría técnica y mentoring son los métodos usados. FBA también se dedica a actividades con organizaciones de la sociedad civil para asegurar la activa y continua participación de mujeres en la construcción de la paz.

Además, la FBA por su amplia experiencia a nivel global, ofrece apoyo en el desarrollo de capacidades en diálogo y mediación.

Con contribuciones de Anna Johansson, Asesora Mujeres, Paz y Seguridad, FBA y Marcelo Díaz, Agregado de Cooperación para Paz y Seguridad Embajada de Suecia en Colombia.

Fotografía:Ejército Nacional de Colombia

BIBLIOGRAFÍA

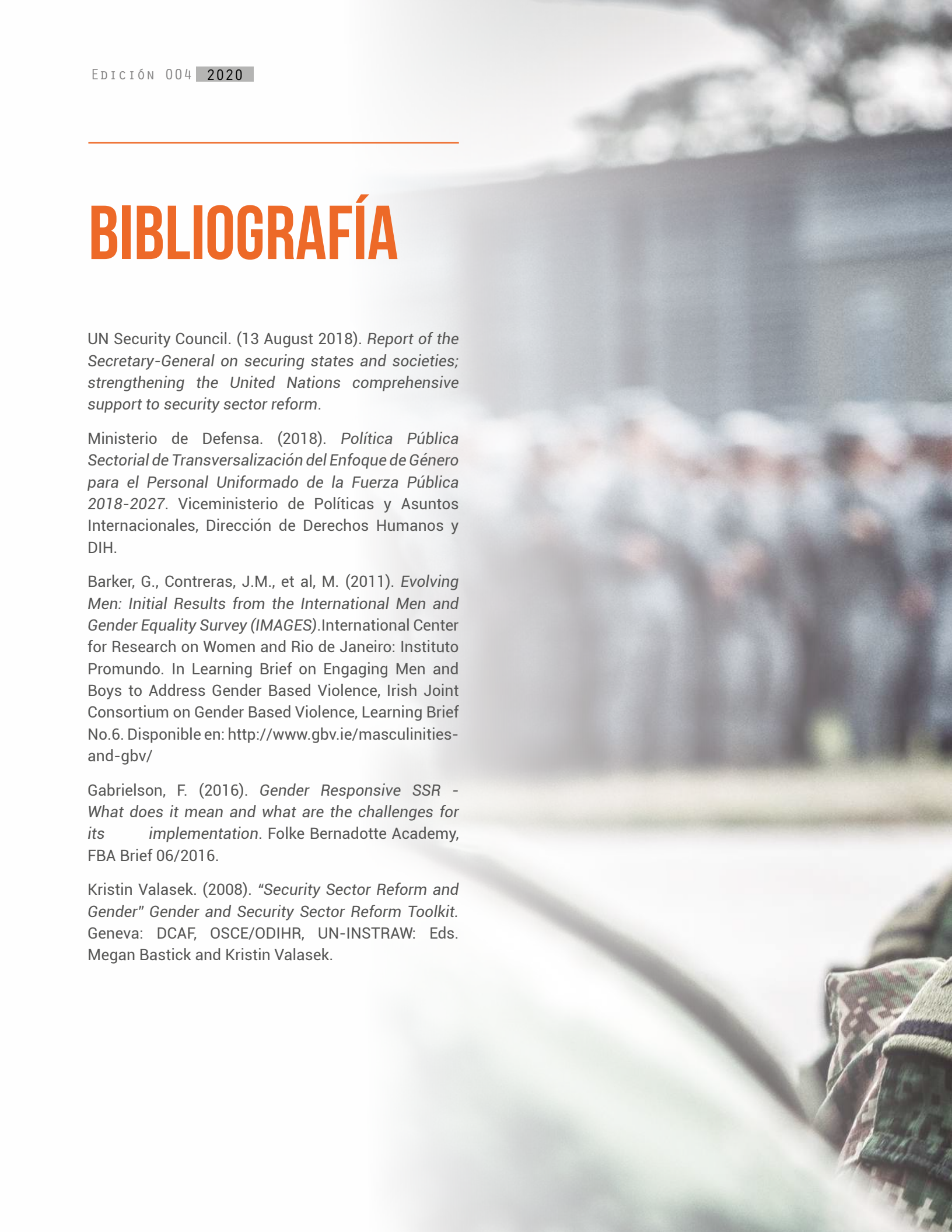
UN Security Council. (13 August 2018). *Report of the Secretary-General on securing states and societies; strengthening the United Nations comprehensive support to security sector reform*.

Ministerio de Defensa. (2018). *Política Pública Sectorial de Transversalización del Enfoque de Género para el Personal Uniformado de la Fuerza Pública 2018-2027*. Viceministerio de Políticas y Asuntos Internacionales, Dirección de Derechos Humanos y DIH.

Barker, G., Contreras, J.M., et al, M. (2011). *Evolving Men: Initial Results from the International Men and Gender Equality Survey (IMAGES)*.International Center for Research on Women and Rio de Janeiro: Instituto Promundo. In Learning Brief on Engaging Men and Boys to Address Gender Based Violence, Irish Joint Consortium on Gender Based Violence, Learning Brief No.6. Disponible en: http://www.gbv.ie/masculinities-and-gbv/

Gabrielson, F. (2016). *Gender Responsive SSR - What does it mean and what are the challenges for its implementation*. Folke Bernadotte Academy, FBA Brief 06/2016.

Kristin Valasek. (2008). *"Security Sector Reform and Gender" Gender and Security Sector Reform Toolkit.* Geneva: DCAF, OSCE/ODIHR, UN-INSTRAW: Eds. Megan Bastick and Kristin Valasek.



Fotografía:Ejército Nacional de Colombia

EL AVANCE DE LA TECNOLOGÍA MILITAR Y LA INTELIGENCIA ARTIFICIAL: UN ANÁLISIS DE LOS DESAFÍOS EMERGENTES DEL USO DE LA FUERZA POR MEDIO DE SISTEMAS AUTÓNOMOS

Anna Caroline Pott

Realizó una maestría en el Programa de Postgrado en Estudios Marítimos de la Escuela de Guerra Naval y en Programa de Postgrado en Políticas Públicas, Estrategias y Desarrollo del Instituto de Economía de la Universidad Federal de Río de Janeiro. Becaria del Club Naval. Licenciada en Ciencias De la Universidad Federal de Río de Janeiro.

RESUMEN

Al discutir el futuro de las tecnologías militares, Eliot Cohen hace referencia a tres sectores de creciente y especial relevancia: el espacio, el ciberespacio y la industria manufacturera, representada por la nanotecnología, la robótica y la inteligencia artificial (Cohen, 2013). Estas tecnologías reflejan el deseo humano por la creación de sistemas cada vez más eficientes, inteligentes y autónomos. Su desarrollo

se justificaría en la medida en que la humanidad vive en un entorno cada vez más complejo, donde la sobrecarga y velocidad de la información de los conflictos modernos pueden generar confusión y comprometer la eficacia de la respuesta humana. Por consiguiente, sería necesaria la creación de sistemas capaces de recopilar y analizar la información de forma rápida y dinámica.

Dichos desarrollos tecnológicos han incentivado que el ser humano empiece a ser un observador (man-out-of-the-loop) de operaciones militares que involucran directamente el uso de la fuerza, lo cual ha generado fuertes cuestionamientos y críticas, dados los alcances e impactos desmedidos que el uso y creación de sistemas autónomos pueden tener. Como ejemplo, se cita el empleo de drones en operaciones militares en Pakistán, Somalia y Yemen.

Analizar el avance de las tecnologías militares, a partir del desarrollo de la inteligencia artificial, es importante, una vez que científicos en los más diversos laboratorios del mundo ya están trabajando en nuevas tecnologías que desempeñarán un papel importante en el período denominado posthuman war. En este sentido, Christopher Coker resalta que tecnologías como cyber robots, nanotecnologías e ingeniería genética tendrán gran relevancia en la transformación de los conflictos, al disminuir el papel del ser humano (Coker, 2012). Es así como este trabajo tiene como objetivo identificar los desafíos derivados del desarrollo y empleo de las tecnologías militares emergentes en el campo de la inteligencia artificial. La metodología empleada en el estudio es la exploratoria, por medio de la revisión bibliográfica escogida.

Palabras clave: *Tecnologías militares, inteligencia artificial, aviones no tripulados, sistemas autónomos, Derecho Internacional de los Conflictos Armados, ética.*

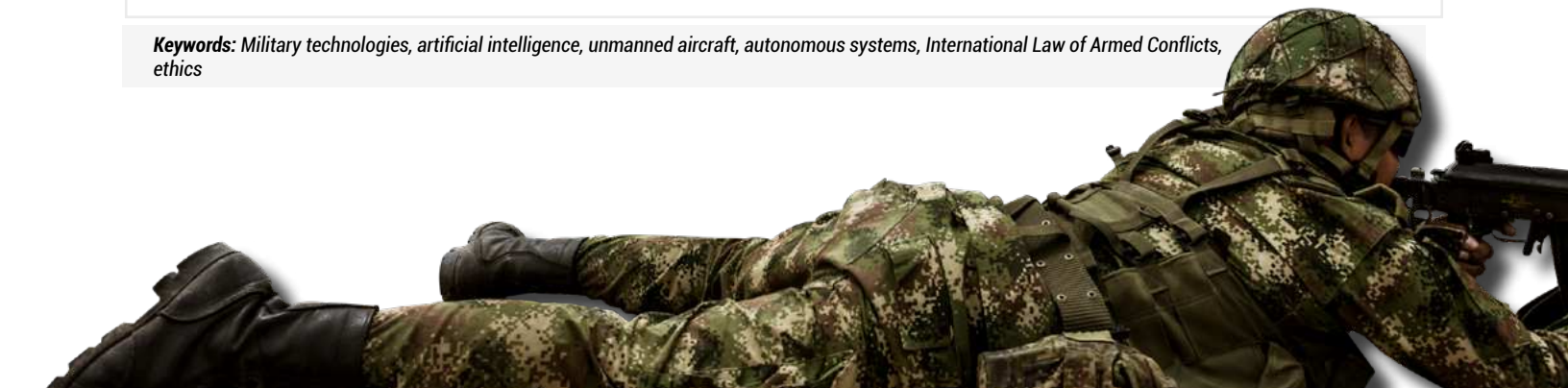
ABSTRACT

When discussing the future of military technologies, Eliot Cohen refers to three sectors of growing and special relevance: space, cyberspace and manufacturing, represented by nanotechnology, robotics and artificial intelligence (Cohen, 2013). These technologies reflect the human desire for the creation of increasingly efficient, intelligent and autonomous systems. The development of these technologies would be justified to the extent that humanity lives in an increasingly complex environment, where the overload and speed of the information of modern conflicts can generate confusion and compromise the speed and efficiency of the human response. Therefore, it would be necessary to create systems capable of collecting and analyzing information quickly and dynamically.

These technological developments have encouraged the human begin being an observer (man-out-of-the-loop) of military operations that directly involve the use of force, which has generated strong questions and criticisms, given the scope and excessive impacts that the use and creation of autonomous systems can have. As an example, the use of drones in military operations in Pakistan, Somalia and Yemen is cited.

Analyzing the progress of military technologies, from the development of artificial intelligence, is important, once scientists in the most diverse laboratories of the world are already working on new technologies that will play an important role in the period called posthuman war. In this sense, Christopher Coker highlights that technologies such as cyber robots, nanotechnologies and genetic engineering, will have great relevance in the transformation of conflicts, by diminishing the role of the human being (Coker, 2012). This is how this work aims to identify the challenges arising from the development and use of emerging military technologies in the field of artificial intelligence. The methodology used in the study is exploratory, through the selected literature review.

Keywords: *Military technologies, artificial intelligence, unmanned aircraft, autonomous systems, International Law of Armed Conflicts, ethics*



Al discutir el futuro de las tecnologías militares, Eliot Cohen hace referencia a tres sectores de creciente y especial relevancia: el espacio, el ciberespacio y la industria manufacturera, representada por la nanotecnología, la robótica y la inteligencia artificial (Cohen, 2013). Estas tecnologías reflejan el deseo humano por la creación de sistemas cada vez más eficientes, inteligentes y autónomos.

Su desarrollo se justifica en la medida que la humanidad vive en un ambiente cada vez más complejo, donde la sobrecarga y la velocidad de la información, que caracteriza los conflictos modernos, pueden generar confusión y comprometer la eficacia de la respuesta humana a estos fenómenos. Por ello, se plantea necesaria la creación de sistemas capaces de recopilar y analizar la información de forma rápida y dinámica, para preservar infraestructuras y vidas humanas. La idea es que estos sistemas tengan la capacidad de reducir posibles fallas cognitivas, así como la influencia negativa que tiene el hombre sobre la tecnología.

Dichos desarrollos tecnológicos han incentivado que el ser humano empiece a ser un observador (man-out-of-the-loop) de operaciones militares que involucran directamente el uso de la fuerza, lo cual ha generado fuertes cuestionamientos y críticas, dados los alcances e impactos desmedidos que el uso y creación de sistemas autónomos pueden tener. Sin embargo, Cohen afirma que el ser humano no abandonará por completo su rol en el teatro de operaciones, a pesar de existir una fuerte tendencia por parte del hombre para desarrollar máquinas inteligentes y autónomas que enfrenten a los enemigos indeseables (Cohen, 2013).

De acuerdo con este autor, el uso de tales tecnologías traerá una serie de dificultades para las fuerzas convencionales, incluyendo la toma de decisiones en el campo militar. Estas dificultades se traducen no sólo en desafíos para las fuerzas armadas, sino también para la sociedad, en tanto el empleo de nuevas tecnologías en el teatro de operaciones puede contraponerse a los derechos humanos y al derecho internacional humanitario. Ejemplo de ello, puede ser el empleo de drones en operaciones militares en Afganistán, Pakistán, Somalia y Yemen.

El desarrollo de tecnologías en el área de la inteligencia artificial ya puede ser encontrado en algunos sectores civiles, como, por ejemplo, el jurídico (The Atlantic, 2017). A propósito, cabe resaltar la creación de Ross, el robot-abogado, diseñado por la Universidad de Toronto, a partir de la tecnología de Watson, máquina

Fotografía:Ejército Nacional de Colombia

de inteligencia cognitiva desarrollada por IBM -International Business Machines-. En comparación con el ser humano, Ross tiene una capacidad única de almacenamiento, ya que puede procesar 500 gigabytes de información en sólo un segundo. El uso de una máquina de estas implica una ventaja competitiva, teniendo en cuenta que el robot-abogado es una fuente de consulta avanzada, capaz de adquirir nuevos conocimientos rápidamente, almacenarlos e informárselos a los abogados en aquellos escenarios donde puedan ser afectados los casos en progreso.

En el ámbito civil y militar, la inteligencia artificial ya es tenida en cuenta para el desarrollo de estudios legales y filosóficos. A propósito, Christopher Coker destaca que las tecnologías estarían llevando a la humanidad al período denominado posthuman war, en el que se hace necesario prestar atención a los desarrollos tecnológicos y su efecto directo en la evolución del pensamiento militar (Coker, 2012).

Analizar el avance de las tecnologías militares a partir de la inteligencia artificial es importante, una vez que científicos en los más diversos laboratorios del mundo ya están trabajando en nuevas tecnologías que desempeñarán un papel importante en el periodo posthuman war. Al igual que Cohen, Coker afirma que tecnologías como los cyber robots, nanotecnologías e ingeniería genética, tendrán un rol fundamental en la transformación del conflicto, disminuyendo el rol del ser humano y demandando la revisión y creación de nuevos conceptos que reflejen esa realidad (Coker, 2012).

EL CRECIMIENTO DE LOS SISTEMAS AUTÓNOMOS: CONCEPTO Y PERSPECTIVA HISTÓRICA

En la publicación *Unmanned Aerial Vehicles for Maritime Patrol: Human Factors Issues* se identificaron distintos niveles de automatización que varían a lo largo de dos ejes perpendiculares, como se presenta en la Figura No.1. En el eje vertical se mide la capacidad de procesamiento de informaciones, la toma de decisión y la resolución de problemas por parte del sistema, mientras que, en el eje horizontal, se mide la autonomía de vuelo. Entre mayores sean los niveles de capacidad decisoria y de autonomía por parte del sistema de vuelo, los recursos cognitivos y sensoriales exigidos por parte del operador serán menores.

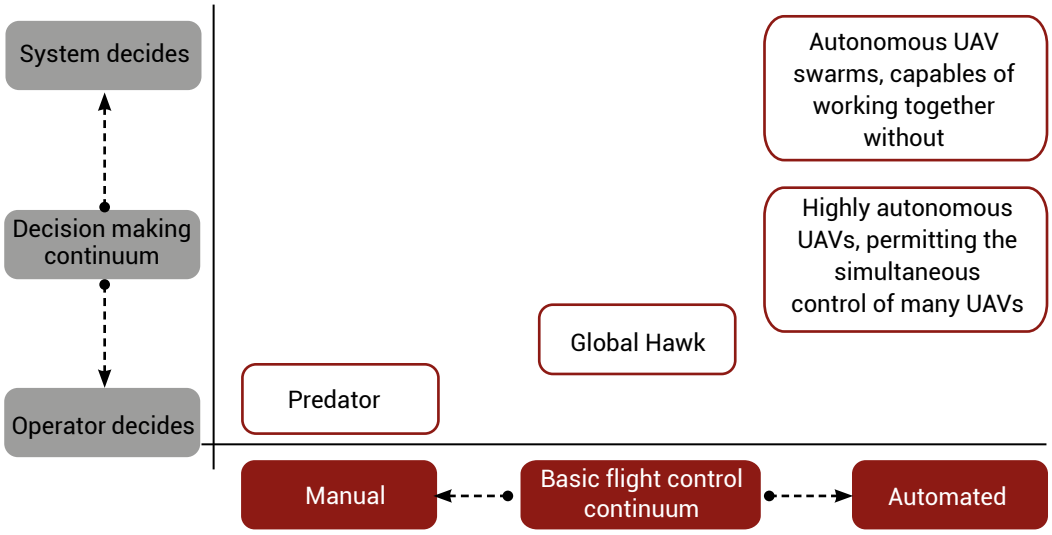


Figure 1. **Niveles de autonomía** Fuente: Hopcroft et al., 2006

La representación gráfica trae como ejemplo de sistemas parcialmente autónomos el *Predator* y el ***Global Hawk.*** Ambos pueden ser clasificados como plataformas remotamente operables. En un nivel superior estarían los sistemas crecientemente autónomos, con capacidad de operabilidad simultánea, y, por encima de éstos, estarían los sistemas autónomos con capacidad de trabajo en equipo, sin monitoreo humano. Las dos últimas categorías aún no existen en su plenitud, aunque ya se registran proyectos que han encaminado esfuerzos para lograrlo.

En el léxico del Ejército estadounidense, plataforma o vehículo remotamente operable significa "un vehículo no tripulado capaz de ser controlado a distancia a través de un enlace de comunicación" (US Army, 2005).

Los vehículos remotamente operables pueden ser terrestres, marítimos, submarinos, subterráneos y aéreos. De esta forma, cualquier máquina puede ser "dronizada", siempre y cuando no haya humanos a bordo:

> Un dron puede ser controlado a distancia, por operadores humanos - principio de mando a distancia -, ya sea de forma autónoma o por dispositivos robóticos - principio de pilotaje automático. En la práctica, los drones actuales combinan estos dos modos de control. Los ejércitos todavía no disponen de "robots letales autónomos" operativos, aunque (…) existen proyectos avanzados en ese sentido (Chamayou, 2015).

Los drones se popularizaron en el ambiente aéreo y son conocidos oficialmente como vehículo aéreo no tripulado – *unmanned aerial vehicle, UAV*- o vehículo de combate no tripulado -*unmanned combat air vehicle, UCAV*-. Esta clasificación depende del empleo o no de armamento. Los vehículos aéreos no tripulados se utilizan para la vigilancia, el reconocimiento y la cartografía; por su parte, los vehículos no tripulados armados (drones cazadores) son capaces de conducir ataques informados a través de medios de alcance internacional. La conversión de estas dos máquinas (de vigilancia y de combate) ya existe y se ve materializada en una ventaja en el campo de batalla, ya que son sistemas que pueden proyectar su ataque a distancia desde el aire. Se aniquila al enemigo a la distancia antes de que él pueda hacer lo mismo (Chamayou, 2015).

Fotografía:Ejército Nacional de Colombia

Se resalta que, desde la Primera Guerra Mundial (1914-1918), ya se experimentaba el empleo de aviones con cámaras, que permitían el reconocimiento del territorio y el monitoreo del enemigo (Peron & Borelli, 2014). Otras iniciativas como el *Curtiss-Sperry Aerial Torpedo* y el *Kettering Bug* y, además, los *V-1* y *V-2* nazis pueden ser considerados como precursores de los misiles de crucero, que apuntaban a desarrollar iniciativas ligadas al posterior desarrollo de los drones.

La inversión en drones ocurrió por primera vez durante las operaciones militares estadounidenses en Vietnam. En la época, se invirtió en drones de reconocimiento, conocidos como *Lightning Bugs* de la empresa *Ryan Aeronautical* (Chamayou, 2015). Se trata de un cambio en el escenario de conflicto, teniendo en cuenta que las tripulaciones estaban protegidas de los ataques. Sin embargo, tras el fin de la guerra, la inversión fue abandonada en los EE.UU., y sólo se mantuvo en pocos países, como Israel.

Las inversiones estadounidenses en drones regresaron entre los años 1980 y 1990 con ayuda del perfeccionamiento de las tecnologías de información y comunicación. En ese periodo, los vehículos aéreos no tripulados se utilizaron para el reconocimiento, la vigilancia y la cartografía. El paso para el uso de drones con empleo de armamento se produjo entre Kosovo y Afganistán, con el prototipo del avión espía teledirigido *Predator*, desarrollado por la empresa *General Atomics*:

> La utilización de los UAV se intensificó principalmente tras la intervención de la Organización del Tratado del Atlántico Norte (OTAN) en Kosovo y posteriormente en las campañas de Afganistán e Irak bajo la forma de los drones, que, como se ha visto, incorporan no sólo sistemas de cámaras y sensores para vigilancia y reconocimiento, sino también sistemas de armas (Peron & Borelli, 2014).

Los drones provistos de armamentos pasaron a ser utilizados con más frecuencia en la guerra contra el terror iniciada por EE.UU. tras el atentado terrorista del 11 de septiembre de 2001. Su empleo creció de modo que en 2015 las fuerzas armadas estadounidenses poseían aproximadamente seis mil drones de diversos tipos, englobando drones de la fuerza aérea, ejército y marina (USA, 2012).

De esta manera, ataques de drones se convirtieron en rutinarios en países como Afganistán, Pakistán, Somalia y Yemen. En Pakistán se estimó que un ataque con dron se producía cada cuatro días (The Bureau Investigates, 2017). En ese mismo país, se estimaron más de tres mil muertos de 2004 a 2015 (The Bureau Investigates, 2017) por ataques de drones. Se observó, además, que hubo un aumento en el número de este tipo de ataques y este tipo de muertes del gobierno Bush al gobierno de Obama.

En ese contexto, se observó que hubo un aumento del 1.200% en el patrullaje de drones estadounidenses (The Economist, 2017). Tal aumento explicó el incremento en la formación de pilotos de drones en comparación con pilotos de aviones de combate y bombardeo convencionales (The NY Times, 2017). Cabe resaltar en este punto que la formación de pilotos de vehículos aéreos remotamente operables pone en cuestión el involucramiento de las emociones humanas en el teatro de operaciones, pues se ha evidenciado que el ejecutor no se siente emocionalmente involucrado con su enemigo al momento de adelantar la ejecución del ataque.

Teniendo en cuenta la necesidad de perfeccionar las armas militares, el ser humano busca la creación y el desarrollo de armamentos más letales y eficaces, disminuyendo costos de operaciones militares y haciéndolas más seguras para sus combatientes. Se pretende, así, dar inicio a la creación de sistemas cada vez más autónomos.

A diferencia de las plataformas remotamente operables o de sistemas automatizados, los sistemas autónomos son aquellos que dictan “las propias reglas de conducta de forma independiente de terceros, o, si queremos, desde una perspectiva del ciclo de decisión, es capaz de observar, orientar, decidir y “actuar sin asistencia humana externa” (Vicente, 2013). Por lo tanto:

> Un sistema automatizado sigue un conjunto de instrucciones para completar una tarea de forma previsible, mientras que un sistema autónomo puede reaccionar de forma adaptativa a eventos inesperados, apenas viendo limitadas sus opciones de respuesta por un conjunto de reglas básicas, preinstaladas en su sistema (Vicente, 2013).

"TENIENDO EN CUENTA LA NECESIDAD DE PERFECCIONAR LAS ARMAS MILITARES, **EL SER HUMANO BUSCA LA CREACIÓN Y EL DESARROLLO** DE ARMAMENTOS MÁS LETALES Y EFICACES, DISMINUYENDO COSTOS DE OPERACIONES MILITARES Y HACIÉNDOLAS **MÁS SEGURAS PARA SUS COMBATIENTES**. SE PRETENDE, ASÍ, DAR INICIO A LA CREACIÓN DE SISTEMAS **CADA VEZ MÁS AUTÓNOMOS."**

El desarrollo y la consiguiente construcción y producción de sistemas autónomos se enfrentan principalmente con dos obstáculos: la capacidad tecnológica y la aceptación de la sociedad para su empleo. Con respecto a este último, se destaca que se trata de una temática difundida constantemente por los medios de comunicación internacionales. En el ámbito internacional, las noticias apuntan que expertos en el tema discuten cómo el derecho internacional humanitario puede regular las tecnologías emergentes en el área de inteligencia artificial (Australian Science, 2017). Además, se encuentran en los medios de comunicación noticias que apuntan a los peligros del uso de drones, incluso como actividad de ocio (BBC, 2017).

En el mismo sentido, movimientos sociales en contra de los drones se disiparon por las redes sociales. La Organización de las Naciones Unidas (ONU), en atención a la temática, abrió investigaciones sobre el uso de la fuerza a través de plataformas remotamente operables en el ámbito del Consejo de Derechos Humanos (The Guardian, 2017).[1]

De esta forma, se observa que el debate sobre plataformas remotamente operables y sistemas autónomos son cuestiones políticas realmente polémicas que merecen atención del Estado y de la sociedad. En vista de las implicaciones éticas, morales, políticas y legales, se hace necesario desarrollar un análisis y un debate sobre el uso de tales tecnologías en las operaciones militares que involucren directamente el uso de la fuerza. Tal debate se hace necesario antes de la creación, el desarrollo y el empleo de sistemas cada vez más autónomos, teniendo en cuenta que tales tecnologías pueden ser potencialmente devastadoras.

DESAFÍOS DERIVADOS DEL USO DE LA FUERZA POR MEDIO DE PLATAFORMAS REMOTAMENTE OPERABLES Y SISTEMAS AUTÓNOMOS

A partir del desarrollo y uso de la fuerza a través de plataformas remotamente operables y sistemas autónomos se plantean desafíos tecnológicos, políticos, éticos, morales y legales. A pesar de ello, el Departamento de Defensa de Estados Unidos se empeña en reducir la acción humana en los drones, encaminándose hacia una autonomía total, donde el ser humano pasa a ser sólo observador de operaciones militares. En ese sentido, Peter W. Singer prevé la "dronización" de las fuerzas armadas estadounidenses a mediano plazo (Singer, 2011).

En cuanto a las dificultades de la creación de este tipo de tecnologías, éstas se presentan en el (a) procesamiento de información en tiempo real, (b) obstáculos al momento de simular enfrentamientos que pueden suceder en el mundo real, así como (c) la inexistencia de protocolos comunes que conduzcan a la interoperabilidad, lo cual dificulta la implementación de sistemas autónomos (Weiss, 2011). A pesar de dichas dificultades, se cree que en la medida en que las necesidades operativas de los ejércitos del mundo aumenten, dichos obstáculos serán superados (Vicente, 2013).

[1] El ponente especial sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo, Ben Emmerson, ha presentado algunos informes sobre la temática.

Fotografía:Ejército Nacional de Colombia

En el aspecto político, se observa que el uso de la fuerza, por medio de plataformas remotamente operables y sistemas autónomos, asegura menores costos y restricciones. Sin embargo, la sociedad constituye una barrera al libre desarrollo e implementación de esas tecnologías en el campo de batalla. Los medios internacionales a diario transmiten noticias sobre las ejecuciones selectivas cometidas por la Central Intelligence Agency (CIA), lo cual ha abierto debates en variados niveles de la sociedad, además de aumentar los niveles de desconfianza en el uso de dichas tecnologías.

Aunque, por su bajo costo en términos operativos, las plataformas remotamente operables y sistemas autónomos permiten una mayor opción estratégica, además de flexibilizar el aparato militar con recursos civiles (Vicente, 2011), el riesgo se halla en el empleo de la fuerza como primera opción, ya que podría aumentar la frecuencia del número de conflictos con consecuencias potencialmente destructivas. En el mismo sentido, Krishnan hace referencia a los riesgos de proliferación del uso de esas tecnologías, incluso por parte de actores no estatales:

“Aunque, por su bajo costo en términos operativos, las plataformas remotamente operables y sistemas autónomos permiten una mayor opción estratégica, además de flexibilizar el aparato militar con recursos civiles (Vicente, 2011), el riesgo se halla en el empleo de la fuerza como primera opción, ya que podría aumentar la frecuencia del número de conflictos con consecuencias potencialmente destructivas.”

Es muy probable que las armas robóticas puedan proliferar ampliamente e incluso permitir que actores no estatales realicen nuevos tipos de ataques terroristas. La posibilidad de un abuso de tecnologías avanzadas como la robótica, la inteligencia artificial y la nanotecnología por parte de los Estados, incluso democráticos, para la conducción de conflictos internos y de represión política, es ciertamente una preocupación que debe tomarse en serio. También es probable que los estados que tienen armamento robótico de largo alcance puedan comportarse de una forma más agresiva hacia estados que no los poseen. Una gran guerra interestatal podría volver a ser más frecuente, ya sea por el debilitamiento de las restricciones políticas y económicas a la guerra, o por accidentes o desequilibrios precarios de poder (Krishnan, 2009).

En el marco legal se verifica que movimientos individuales y colectivos[2] luchan contra el empleo de plataformas remotamente operables y sistemas autónomos. Tales movimientos piden una reglamentación más asertiva que restrinja el empleo de tales tecnologías, así como protocolos éticos que limiten la acción de las máquinas a nivel del Derecho Internacional de los Conflictos Armados. Hay, incluso, movimientos

[2] Ejemplo de ello son *International Committee for Robot Arms Control* y *Association of Unmanned Vehicle Systems International.*

Fotografía:Ejército Nacional de Colombia

que defienden la completa extinción de drones y el desarrollo de sistemas crecientemente autónomos.

La necesidad de una reglamentación asertiva se hace necesaria, ya que la utilización de drones y sistemas autónomos provocan un desnivel mayor entre los actores estatales y no estatales involucrados en el conflicto. De esta forma, el derecho debe intervenir de forma que pueda evitar el uso de la fuerza indiscriminada y desproporcionada. A propósito, Vicente sostiene la "necesidad de la existencia de un régimen de control de armamento que regule el desarrollo, adquisición y empleo de sistemas de armas autónomas, a fin de restringir la proliferación de plataformas armadas" (Vicente, 2013).

Desde el punto de vista legal, lo importante es que el empleo de plataformas remotamente operables y sistemas autónomos cumplan el Derecho Internacional de los Conflictos Armados y las reglas de compromiso. Requisitos como (a) la necesidad, (b) la humanidad, (c) la distinción y (d) la proporcionalidad deben ser observados en la conducción de un ataque. Sin embargo, en esta materia, siguen surgiendo preguntas, como, por ejemplo: (a) ¿Las reglas existentes, hoy en día, son suficientes para garantizar el uso de dichas tecnologías?, (b) ¿Existe la necesidad de crear un marco legal más asertivo que permita una mayor protección del uso de esta tecnología? (c) ¿Quién es el responsable de los actos legales y posibles fallas derivadas de operaciones desarrolladas con sistemas crecientemente autónomos?

Frente a esta última pregunta surgen nuevos cuestionamientos. En el caso de que un sistema autónomo desobedezca los protocolos de ética incorporados, dos opciones surgen: reprogramación o destrucción de la máquina. Sin embargo, si un humano hiciera caso omiso a la normativa o al protocolo, éste sería juzgado y condenado por su acción. En el caso de los drones, la responsabilidad, aunque todavía oscura, es menos compleja que la de los sistemas autónomos. No obstante, en el caso de los "drones o robots con capacidad de ataque", se abre una ventana más grande en la que el programador y el ingeniero pueden llegar a ser culpables.

Se destaca que las cuestiones de orden tecnológico, político y legal están relacionadas con las cuestiones de orden ético y moral[3]. Se observa, en particular, la conexión que existe entre las cuestiones de orden legal y ético, teniendo en cuenta que el derecho surge para la protección del ser humano, para regir la vida en sociedad de la forma más justa posible. Conforme las costumbres y conductas humanas cambian, el derecho se transforma para poder lidiar con los nuevos tipos de conflictos emergentes.

Vicente destaca que, en el caso de los Estados Unidos de América, las publicaciones del Departamento de Defensa de los Estados Unidos de América casi no abordan las cuestiones éticas y morales del uso de sistemas autónomos (Vicente, 2013). A título de ejemplo, el plan de la Fuerza Aérea de los Estados Unidos para sistemas aéreos no tripulados no menciona detalladamente las cuestiones éticas, exponiendo que las mismas deben ser discutidas brevemente para no impedir el desarrollo continuo de los sistemas autónomos (USAF Fight Plan, 2009).

Frente a la discusión ética, Ronald Arkin es uno de los mayores defensores del uso de sistemas autónomos. Arkin afirma que, en el caso de las máquinas, estas son capaces de actuar con mayor ética que los soldados (Arkin, 2010), comportándose de forma más humana que los propios humanos (Arkin, 2009) y disminuyendo la baja de soldados. Aunque es un fuerte opositor a la guerra, él sostiene que mientras haya conflicto, cree que lo mejor es dejar elevar la carga de la máquina, pero de una manera más precisa y siempre programada para seguir la ley. En este mismo sentido, Peter Olsthoorn destaca que:

> Sistemas no tripulados (especialmente los autónomos, donde el hombre es removido del circuito) son inmunes a la frustración, al aburrimiento y a la rabia. Esto puede hacer que la conducta antiética se presente con menor probabilidad, ya que estas emociones constituyen un factor importante en su ocurrencia. (Olsthoorn, 2011)

En este sentido, los sistemas autónomos poseen la capacidad de reducir las posibles fallas cognitivas, así como reducir la influencia negativa del hombre sobre la tecnología en los casos en que, por ejemplo, el ser humano actúa de forma inadecuada al no respetar los protocolos de guerra y es guiado a partir de emociones como el miedo, la venganza, deseo de victoria. A propósito, Chamayou resalta que estos robots:

Están provistos de lo que él llama un "gobernador moral", una especie de "conciencia" artificial "o de Super-Yo maquínico. Cuando una acción letal es propuesta por otro programa, ese software de deliberación la sometería a la prueba de las leyes de la guerra, traducidas en lógica deóntica "para garantizar que ella constituya una acción éticamente permisible". Los robots, exentos de emociones y de pasiones para perturbar su juicio, son capaces de aplicar reglas textualmente. Esto es porque no "muestran ni miedo, ni rabia, ni frustración, ni venganza"; en otras palabras, son privados de esas propiedades humanas esenciales que llamamos afectos. Se supone que esas máquinas pueden ser más humanas que los humanos, esto es, más éticas, recíprocamente (Chamayou, 2015).

De lo anterior es posible derivar que la implementación de un protocolo ético que sea capaz de regular la letalidad de

[3] Se entiende ética como esencia, carácter, índole. De esta forma, se busca la investigación del ethos, de la propiedad del carácter, tanto el bien como el mal. Se resalta, además, que ética se relaciona con moral, siendo esa última entendida como costumbres necesarias consolidadas en determinada cultura.

"LOS SISTEMAS AUTÓNOMOS POSEEN LA CAPACIDAD DE **REDUCIR LAS POSIBLES FALLAS COGNITIVAS**, ASÍ COMO REDUCIR LA INFLUENCIA NEGATIVA DEL HOMBRE SOBRE LA TECNOLOGÍA EN LOS CASOS EN QUE, POR EJEMPLO, **EL SER HUMANO ACTÚA DE FORMA INADECUADA** AL NO RESPETAR LOS PROTOCOLOS DE GUERRA Y ES GUIADO A PARTIR DE EMOCIONES **COMO EL MIEDO, LA VENGANZA, DESEO DE VICTORIA."**

sistemas autónomos es viable. Tal protocolo de ética atendería los preceptos del Derecho Internacional de los Conflictos Armados y de las reglas de compromiso. Sin embargo, frente a esto surge un desafío: para que una máquina sea capaz de distinguir lo que es justo o injusto, se hace necesario un desarrollo tecnológico concreto y avanzado. Inclusive en los prototipos con mayores niveles de desarrollo tecnológico aún se encuentran dificultades para crear máquinas que estén dotadas de sentido ético y moral. Se resalta que insertar contenido ético y moral dentro de máquinas es una tarea difícil, ya que el ideal y el juicio humano son singulares; sin embargo, Peter Asaro destaca que:

> A medida que las tecnologías robóticas avanzan es posible que éstas adquieran capacidades morales que imiten o reproduzcan las capacidades morales humanas. Mientras que algunos sistemas pueden simplemente promulgar reglas o principios morales preprogramados, los agentes robóticos autónomos pueden ser capaces de formular sus propios principios, deberes y razones, y así hacer sus propias elecciones morales en el sentido más pleno de la autonomía moral. Hay muchas posibilidades para replicar un sujeto moral totalmente autónomo, como agentes con conciencia moral, pero no la libertad de elección para actuar sobre esa conciencia. Mientras que todavía permanece en el campo de la ficción científica, no es imposible, en principio, que un robot pueda alcanzar autonomía en el sentido kantiano, en el que asume responsabilidad por sus acciones y se identifica con la calidad moral de sus propias acciones. En algún punto a lo largo del continuum, pero probablemente antes de la autonomía kantiana, surgirán varios cuestionamientos sobre las responsabilidades morales de los demás con relación a tales sistemas autónomos y, en particular, sobre si esos sistemas tienen derechos y obligaciones morales (Asaro, 2007).

Fotografía:Ejército Nacional de Colombia

Fotografía:Ejército Nacional de Colombia

En el lado opuesto de los defensores de plataformas remotamente operables y sistemas autónomos, está Noel Sharkey. Este autor resalta la dificultad que la máquina tendrá para distinguir combatientes de no combatientes, así como la dificultad en la aplicación de una respuesta proporcional (Sharkey, 2009).

En el escenario de batalla actual, la distinción entre civiles y combatientes es importante, teniendo en cuenta aplicación de las convenciones de guerra. El uso de plataformas remotamente operables y otros sistemas crecientemente autónomos en el espacio urbano se vuelve complicado, ya que estos deberán prever las intenciones y comportamiento del individuo, sin existir aún sensores capaces de realizar tales tareas.

La proporcionalidad de la acción violenta a ser ejecutada también se plantea como obstáculo ético. El ser humano está dotado de juicio, facilitando la aplicación de una respuesta proporcional y justa. La máquina todavía no es capaz de cuantificar el sufrimiento, así como no es capaz de distinguir a los inocentes. Todavía no hay una programación completa y eficiente para la gestión y aplicación de la fuerza letal.

En particular, el distanciamiento del combatiente del escenario de batalla se plantea también como una cuestión moral y ética. Su alejamiento hace que matar se torne más fácil. Los operadores de plataformas remotamente operables se sienten en un juego de videojuegos, en el que el punto máximo es la destrucción del objetivo.

De esta forma, en la visión de Sparrow, las plataformas remotamente operables y los sistemas autónomos no son todavía capaces de cumplir con estándares éticos universales (Sparrow, 2009). Peter Asaro complementa apuntando al hecho de que la ética y moral no están suficientemente explícitas en el reglamento internacional, por lo que deberían implementarse nuevos instrumentos normativos que trabajen la cuestión (Asaro, 2007). Para Sharkey, tales sistemas deberían ser prohibidos, por lo menos hasta que se encuentre una solución a las problemáticas planteadas (Sharkey, 2009).

CONCLUSIONES

Desde su existencia, el ser humano desarrolla herramientas capaces de facilitar su rutina, así como armas destinadas a su protección y existencia. Con el paso de los siglos, el hombre se ha vuelto más inventivo, lo que ha dificultado cada vez más predecir el futuro de sus innovaciones.

Sin embargo, en lo que se refiere al armamento, experiencias pasadas mostraron que se debe tener cuidado en la introducción de un nuevo tipo de sistemas de armas en el teatro de operaciones. Para ello, es necesario evaluar su impacto antes de que pueda alterar significativamente el modus operandi de la guerra y la humanidad.

Se observa que, aunque las nuevas tecnologías impactan el modus faciendi de la guerra, éstas no alteran su esencia. Esto no significa que no haya cambios en la relación de la guerra con la sociedad. Más bien, se resalta que, en lo que se refiere a los aspectos tecnológicos, el desarrollo de la inteligencia artificial puede llevar a la humanidad a un periodo denominado post-humano (*post-human*).

En este sentido, el empleo de sistemas crecientemente autónomos posee ventajas y desventajas. Estos sistemas permiten la reducción del costo en la aplicación y el uso de la fuerza, la flexibilización de las restricciones a lugares de difícil acceso, así como la eliminación de sentimientos como el miedo, la rabia y la frustración del combatiente.

Por lo tanto, en defensa del uso de estos sistemas, podemos destacar que dos de sus finalidades son (i) la preservación de la vida humana, resaltando que se preserva la vida de los nacionales de los Estados poseedores de esa tecnología y (ii) la reducción del costo operativo, aumentando la eficacia de la operación.

Sin embargo, hay aspectos negativos de su uso, tales como (i) los desafíos para distinguir los combatientes de los no-combatientes, (ii) el desafío de la responsabilidad sobre los ataques, así como, (iii) los aún faltantes desarrollos tecnológicos para comprender las intenciones y garantizar la previsión de comportamientos inadecuados por parte de las máquinas, para prevenir el innecesario y desproporcionado uso de la fuerza. Sin duda, tales aspectos negativos impactan en el modus operandi de la guerra.

De esta forma, de acuerdo con la bibliografía investigada, las plataformas remotamente operables y los sistemas autónomos no superan aún los protocolos legales éticos de manera satisfactoria. Las cuestiones legales y éticas surgen, demandando que la comunidad internacional vuelva la discusión en torno a la creación de convenciones de guerra más asertivas que impidan el uso indiscriminado de esas tecnologías, capaces de impactar a la sociedad.

Se destaca, finalmente, que este trabajo tuvo como objetivo reflexionar sobre los desafíos del desarrollo y empleo de tecnologías militares emergentes en el campo de la inteligencia artificial, basándose en la bibliografía de investigación descrita en las referencias. Dada la complejidad de la discusión, no se pretendió agotar la temática. Los desafíos de orden tecnológico, político, social, legal y ética constituyen obstáculos al libre empleo de drones y al desarrollo de sistemas crecientemente autónomos, aunque los mismos no dejen de ser estudiados, desarrollados y utilizados. De los desafíos presentados, muchos cuestionamientos quedan abiertos, constituyendo el próximo paso a ser dado por los estudiosos de la temática.

Fotografía:Ejército Nacional de Colombia

BIBLIOGRAFÍA

ARKIN, R. Ethical Robots in Warfare. Technology and Society Magazine, v. 28, n.1, 2009. Disponível em: < http://www.cc.gatech.edu/ai/robot-lab/online-publications/arkin-rev.pdf>. Acesso em: 20 jun. 2017.

ARKIN, R. The Case for Ethical Autonomy in Unmanned Systems, 2010. Disponível em: <https://smartech.gatech.edu/bitstream/handle/1853/36516/Arkin_ethical_autonomous_systems_final.pdf?sequence=1>. Acesso em: 20 jun. 2017.

ASARO, P. M. How just could a robot war be? Proceedings of the 2008 conference on Current Issues in Computing and Philosophy, p. 50-64, 2008.

Autonomous weapons: an open letter from AI & robotics researchers. Institute of Future of Life, 28 jul. 2015. Disponível em: <http://futureoflife.org/AI/open_letter_autonomous_weapons >. Acesso em: 20 jun. 2017.

BASSO, Brandon et al. Airborne, Autonomous & Collaborative. Mechanical Engineering, April 2011, p. 26-31.

BUMILLER, Elizabeth. A Day Job Waiting for a Kill Shot a World Away. The New York Times, 29 jul. 2012. Disponível em: <http://www.nytimes.com/2012/07/30/us/drone-pilots-waiting-for-a-kill-shot-7000-miles-away.html?_r=0>. Acesso em: 20 jun. 2017.

CHAMAYOU, Grégoire. Teoria do Drone. São Paulo: Cosac Naify, 2015.

Chomsky e Hawking pedem proibição total de armas "inteligentes". Esquerda.net, 02 ago. 2015. Disponível em: <http://www.esquerda.net/artigo/chomsky-e-hawking-pedem-proibicao-total-de-armas-inteligentes/38031>. Acesso em: 20 jun. 2017.

COHEN, Eliot. Technology and warfare. In: BAYLIS, John; WIRTZ, James J.; GRAY, Colin S. Strategy in the contemporary world. 4 ed. New York: Oxford University Press, 2013.

COKER, Christopher. Waging War without Warriors? The Changing Culture of Military Conflict. Colorado: Lynne Riener Publishers, Inc. 2002.

DEVEREAUX, Ryan. UN Inquiry into US Drone Strikes Prompts Cautious Optimism. The Guardian, 24 jan. 2013. Disponível em: <https://www.theguardian.com/world/2013/jan/24/un-announces-drone-inquiry-human-rights>. Acesso em: 20 jun. 2017.

EMMERSON, Ben. Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism. United Nations (General Assembly): A/68/389, Set. 2013. Disponível em: <https://www.justsecurity.org/wp-content/uploads/2013/10/2013EmmersonSpecialRapporteurReportDrones.pdf>. Acesso em: 20 jun. 2017.

Flight of the Drones: Why the Future of Air Power Belongs to Unmanned Systems. The Economist, 8 out. 2011. Disponível em: <http://www.economist.com/node/21531433>. Acesso em: 20 jun. 2017.

HOPCROFT, Robyn et al. Unmanned aerial vehicles for maritime patrol: human factors issues. Australian: DSTO Defence Science and Technology Organisation, 2006.

IBM – International Business Machines. Disponível em: <https://www.ibm.com/br-pt/>. Acesso em: 20 jun. 2017.

KOEBLER, Jason. Rise of the Robolawyers: How legal representation could come to resemble TurboTax. *The Atlantic*, April 2017. Disponível em: <https://www.theatlantic.com/magazine/archive/2017/04/riseoftherobolawyers/517794/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+AtlanticScienceAndTechnology+%28The+Atlantic++Technology%29>. Acesso em: 20 jun. 2017.

KRISHNAN, A. *Killer robots:* Legality and ethicality of autonomous weapons. Surrey: Ashgate, 2009.

LEMOS, Ronaldo. Drones têm falha ética e tecno-

lógica. *Folha de São Paulo*, 02 ago. 2015. Disponível em: <http://www1.folha.uol.com.br/ilustrissima/2015/08/1662855-drones-tem-falha-etica-e-tecnologica.shtml >. Acesso em: 20 jun. 2017.

MATTOSO, Camila. Drone carrega bola para início da final do Campeonato Paulista. *Folha de São Paulo*, 01 maio 2016. Disponível em: <http://www1.folha.uol.com.br/esporte/2016/05/1766727-drone-carrega-bola-para-inicio-da-final-do-campeonato-paulista.shtml>. Acesso em: 20 jun. 2017.

Obama 2013 Pakistan Drone Strikes. *The Bureau of Investigative Journalism*, 3 jan. 2013. Disponível em: <http://www.thebureauinvestigates.com/2013/01/03/obama-2013-pakistan-drone-strikes>. Acesso em: 20 jun. 2017.

OLSTHOORN, P. et al. Risks and Robots: some ethical issues. In: The Ethics of Emerging Military Technologies Seminar, 2011. Proceedings... San Diego, International Society for Military Ethics, 2011.

PERON, A. E. R; BORELLI, P. C. O uso de "drones" pelos Estados Unidos nas operações "targeted killing" no Paquistão e o desrespeito ao Direito Humanitário Internacional: rumo aos estados de violência? Monções: Revista de Relações Internacionais da UFGD, Dourados, v.3. n.6, jul./dez., 2014.

Premiê paquistanês diz que ataque que matou líder Taleban violou soberania. Folha de São Paulo, 22 maio 2016. Disponível em: <http://www1.folha.uol.com.br/mundo/2016/05/1774027-premie-paquistanes-diz-que-ataque-que-matou-lider-taleban-violou-soberania.shtml>. Acesso em: 20 jun. 2017.

Quão seguros são drones? Bebê de 18 meses perde olho ao ser atingido por artefato. BBC Brasil, 04 mar. 2016. Disponível em: <http://www.bbc.com/portuguese/videos_e_fotos/2016/03/160304_video_cego_drone_my>. Acesso em: 20 jun. 2017.

SHARKEY, N. Weapons of indiscriminate lethality. FIfF Kommunikation, 1/09, p. 26-29. 2009.

SINGER, P. W. U-turn. Armed Forces Journal, 9 jun. 2011. Disponível em: <http://www.brookings.edu/research/opinions/2011/04/06-robot-warfare-singer>. Acesso em: 20 jun. 2017.

SPARROW, R. *Killer robots*. Journal of Applied Philosophy, v. 24, n. 1, 2007.

UNITED STATES OF AMERICA. Department of Defense. Dictionary of Military and Associated Terms, Joint Publication 1-2. DoD: 12 Apr. 2001 (As Amended Through 31 Aug. 2005). Disponível em: <http://www.bits.de/NRANEU/others/jp-doctrine/jp1_02(05).pdf>. Acesso em: 20 jun. 2017.

UNITED STATES OF AMERICA. Department of Defense. Report to Congress on Future Unmanned Aircraft Systems, DoD: apr. 2012. Disponível em: <https://www.fas.org/irp/program/collect/uas-future.pdf>. Acesso em: 20 jun. 2017.

USAF FLIGHT PLAN. Unmanned Aircraft Systems Flight Plan 2009-2047. Washington, 2009. Disponível em: < https://fas.org/irp/program/collect/uas_2009.pdf>. Acesso em: 20 jun. 2017.

VICENTE, J. A transformação qualitativa da interferência humana na conduta da guerra. Coleção Meira Mattos, Rio de Janeiro, v.7, n. 30, p. 201-210, set/dez 2013.

VICENTE, J. Da guerra remota – A ascensão dos sistemas aéreos não-tripulados e as implicações para o futuro da conflitualidade hostil. Actas, Observare 1st International Conference, nov. 2011.

WEISS, L. Autonomous Robots in the Fog of War. IEEE Spectrum, august/2011. Disponível em: <http://spectrum.ieee.org/robotics/military-robots/autonomous-robots-in-the-fog-of-war>. Acesso em: 20 jun. 2017.

WELSH, Sean. World split on how to regulate 'killer robots'. Australian Science, 2016. Disponível em: <http://www.australasianscience.com.au/article/scienceandtechnology/worldsplithowregulatekillerrobots.html>. Acesso em: 20 jun. 2017.

WOODS, Chris. Drone Strikes Rise to One Every Four Days. The Bureau of Investigative Journalism, 18 jul. 2011. Disponível em: <http://www.thebureauinvestigates.com/2011/07/18/us-drone-strikes-rise-from-one-a-year-to-one-every-four-days>. Acesso em: 20 jun. 2017.

EL SISTEMA INTEGRADO DE MONITOREO DE FRONTERAS (SISFRON): FACTOR DE INDUCCIÓN DE CAPACIDADES OPERATIVAS AL EJÉRCITO BRASILEÑO

Coronel Sergio Dos Santos Botelho

Coronel de Caballería del Ejercito brasileño, profesional en ciencias militares, magister en operaciones militares. Dentro de su trayectoria se ha desempeñado la función de Comandante del 3er Batallón de Aviación del Ejército, además las funciones de Asesor Técnico de la Cooperación Militar en el campo de la Aviación del Ejército, entre Brasil y Bolivia, Jefe de la Sección 3ª del Comando Militar del Oeste y Jefe de la Sección de Investigación y Prevención de Accidentes Aeronáuticos del Comando de Operaciones Terrestres. Fue alumno del Curso de Altos Estudios Militares CAEM 2019.

RESUMEN

Con base en las orientaciones de la Política Nacional de Defensa (PND) y Estrategia Nacional de Defensa (END), inicialmente emitidas en 2005 y 2008, respectivamente, el Ejército Brasileño emitió en 2010 la Directiva para la implantación del proyecto Sistema Integrado de Monitoreo de Fronteras

(SISFRON) con la finalidad de dotar a la Fuerza de los medios necesarios para ejercer el monitoreo y control, continuo y permanente, de áreas de interés del territorio nacional, particularmente de la franja de frontera terrestre brasileña. El presente artículo realiza la descripción de las principales funcionalidades del Sistema e identifica cómo ese ambicioso proyecto indujo nuevas capacidades operativas, contribuyendo de forma efectiva al Proceso de Transformación del Ejército de Brasil.

Palabras clave: *SISFRON, Fronteras, Transformación, Estrategia Militar, Interagencial*

ABSTRACT

Based on the guidelines of the National Defense Policy (NDP) and National Defense Strategy (NDS), initially issued in 2005 and 2008 respectively, the Brazilian Army issued in 2010, the Directive for the implementation of the project Integrated Monitoring System of Borders (SISFRON) with the purpose of providing the Force with the necessary means to exercise continuous and permanent monitoring and control of areas of interest in the national territory, particularly in the Brazilian border area. This article describes the main functionalities of the System and seeks to identify how this ambitious project induced new operational capabilities, contributing effectively to the Process of Transformation of the Brazilian Army.

Keywords: *SISFRON, Borders, Transformation, Military strategy*

INTRODUCCIÓN

Considerado como uno de los principales proyectos etratégicos del Ejército brasileño, el Sistema Integrado de Monitoreo de Fronteras (SISFRON) fue concebido para efectuar el monitoreo, control y actuación en las fronteras terrestres, con la finalidad de promover la inviolabilidad del territorio nacional, reducir los problemas provenientes de la región fronteriza y fortalecer la interoperabilidad, las operaciones interagenciales y la cooperación regional para la vigilancia de fronteras (Exército Brasileiro, 2012).

El perfil brasileño -al mismo tiempo continental y marítimo, ecuatorial, tropical y subtropical, de larga frontera terrestre con casi todos los países sudamericanos y de amplio litoral y aguas jurisdiccionales- confiere al país profundidad geoestratégica y hace compleja la tarea de la planificación general de defensa (Ministério da Defesa. PND, 2012).

Esta peculiar fisiografía, con aproximadamente 8,5 millones de kilómetros cuadrados de superficie, certifica al país una frontera terrestre con cerca de 17 mil kilómetros de extensión, lo que corresponde al 27% del territorio nacional, que incluye 11 departamentos fronterizos y está dispuesta por 10 países vecinos. Además, hay 32 ciudades gemelas[1] en la frontera terrestre brasileña (Gabinete de Segurança Institucional, 2018).

Se entiende como Capacidad la aptitud requerida a una fuerza o organización militar, para que pueda cumplir determinada misión o tarea. Y según lo conceptuado en el Catálogo de Capacidades del Ejército (2015, pág. 7), la capacidad militar terrestre está constituida por un grupo de capacidades operativas[2] con conexiones funcionales, reunidas para que sus desarrollos potencien las aptitudes de una fuerza.

En este sentido, el SISFRON tiene entre sus objetivos garantizar la superioridad de información, a través del empleo de tecnologías avanzadas, a fin de proporcionar a los comandantes, en diversos escalones, la conciencia situacional necesaria para actuar e intervenir con oportunidad en las operaciones desarrolladas en la franja de frontera, generando así capacidades operativas necesarias para el combate de la era del conocimiento[3] (Estado-Maior, 2017).

[1] Las ciudades gemelas son aquellas en las que el territorio del municipio limita con el país vecino y su sede se ubica en el límite internacional, pudiendo o no presentar una conurbación con una localidad del país vecino (CDIF, 2010).

[2] Es la aptitud requerida a una fuerza u organización militar, para que puedan obtener un efecto estratégico, operacional o táctico. Se obtiene a partir de un conjunto de siete factores determinantes, interrelacionados e indisociables: Doctrina, Organización (y/o procesos), Adiestramiento, Material, Educación, Personal e Infraestructura - que forman el acrónimo DOAMEPI (Estado-Maior, 2015).

[3] Presupone una Fuerza que debe ser dotada de armamentos y de equipos con alta tecnología agregada, sustentada por una doctrina en constante evolución, integrada por recursos humanos altamente entrenados y motivados. Para ello, basa su organización en estructuras con las características de flexibilidad, adaptabilidad, modularidad, elasticidad y sostenibilidad, que permiten alcanzar resultados decisivos en las Operaciones en el Amplio Espectro, con prontitud operativa, y con capacidad de empleo del poder militar de forma gradual y proporcional a la amenaza (Estado-Maior, 2013).

Fotografía: http://www.eb.mil.br/

El SISFRON fue concebido por iniciativa del Comando del Ejército, como consecuencia de la aprobación de la Estrategia Nacional de Defensa, en 2008, que orienta la organización de las Fuerzas Armadas bajo la égida del trinomio monitoreo/ control, movilidad y presencia. El sistema enfatiza la densificación de Unidades de las Fuerzas Armadas en las fronteras e impulsa la capacitación de la industria nacional para la conquista de la autonomía en tecnologías indispensables a la defensa (CCOMSEx, 2012).

La concepción general y la planificación inicial del Sistema constan de su Proyecto Básico, que fue elaborado en 2010 y 2011, mediante contratación de empresas nacionales con experiencia en la integración de proyectos complejos y de gran amplitud. En conjunto, los Órganos de Asesoramiento Inmediato del Comandante, las Subjefaturas del Estado Mayor del Ejército, los Órganos de Dirección Sectorial y los Mandos Militares de Área involucrados participaron en el proceso de elaboración del Proyecto Básico, a través de reuniones de integración, encuentros técnicos y multidisciplinares, visitas técnicas, grupos de trabajo y otras formas de interacción (CCOMSEx, 2012).

Según a la directiva del Estado Mayor del Ejército (2017, pág. 74), el SISFRON deberá comprender cuatro vertientes que viabilizarán las funcionalidades pretendidas por el Sistema:

A. Detección - se traduce en la generación de capacidad de monitoreo para la adquisición de datos en la franja de frontera, contribuyendo en el control efectivo de esas áreas y atendiendo a la directriz estratégica de monitoreo/control constantes de la Estrategia Nacional de Defensa. Se compondrá de diversos subsistemas que tendrán como función preponderante el aumento de la amplitud, calidad y profundidad de la observación y emisión de la alerta temprana acerca de posibles amenazas;

B. Apoyo a la decisión - la estructura facilitará la generación de la información, la integración de datos y el ejercicio de mando y control sobre las diversas actividades en la frontera terrestre de Brasil, viabilizando una conciencia situacional para apoyar al decisor en los niveles necesarios. Aquí se materializa la función de combate comando y control con sus

tres vertientes: la autoridad, la infraestructura y los procesos. Los datos generados alimentarán los sistemas informatizados, que servirán de base para la planificación de acciones militares o, aún, la actuación de otros organismos gubernamentales;

C. Apoyo a la actuación - comprende, en coordinación con otras iniciativas, la adquisición de todos los sistemas y materiales de empleo militar, así como toda la infraestructura física, necesaria para la planificación, la actuación y el seguimiento de las operaciones militares; y

D. Obras de infraestructura - tiene por objeto dotar a las organizaciones militares de las estructuras físicas de almacenamiento, protección y apoyo logístico adecuados a los nuevos medios de empleo militar a ser provistos por el Sistema, así como a edificar las construcciones destinadas a albergar unidades militares creadas debido a las demandas de funcionamiento del Sistema.

El Proyecto Básico indica que el SISFRON debe tener la capacidad de cumplir todo el ciclo de C², de los sensores a los actuadores (fuerzas), posibilitando a los comandantes alcanzar superioridad informacional que posibilite decidir con oportunidad y acierto. En suma, el SISFRON es un sistema centrado en redes, cuyo objetivo es apoyar el proceso decisorio de los comandantes. Tomando la decisión, el sistema posibilitará el accionamiento inmediato de los actuadores para el cumplimiento de la misión (Silveira, 2017). Con el fin de obtener una mejor comprensión, Silveira (2017, pág. 63) detalla las principales divisiones de los subsistemas SISFRON:

- El de detección, en Ópticos y Optrónicos para dotar a las Organizaciones Militares (OM) con medios de observación directa (binoculares, visores nocturnos y termales, etc.).

- Vigilancia, Monitoreo y Reconocimiento (SVMR) para dotar a las OM de medios y observación indirecta (radares de vigilancia terrestre y cámaras de largo alcance). De Medidas de Apoyo de Guerra Electrónica (MAGE) para posibilitar el sensor de emisiones electromagnéticas.

- Las comunicaciones tácticas (ComTat) para proporcionar conexiones al mando de las OM.

- Comunicaciones Estratégicas (ComEstr) para realizar el transporte de la información en redes de alta capacidad (backbone).

- El de Comunicaciones Satelitales (ComSat) para dar flexibilidad al sistema con la utilización del componente espacial.

Fotografía: http://www.eb.mil.br/

La defensa de la patria es la destinación premeditada de las Fuerzas Armadas. La misión de la Fuerza Terrestre en la franja de frontera es contribuir a la defensa de la Patria, atendiendo, de forma eficaz y efectiva, las directrices constantes en la Estrategia Nacional de Defensa. En este sentido, la adopción de un sistema de monitoreo, detección y apoyo a la decisión en la franja de frontera permitirá a la Fuerza Terrestre potenciar las actuales Capacidades Operativas de las tropas ya instaladas o empleadas en esa franja del territorio nacional, ya sea en el cumplimiento de su misión constitucional, así como actuando en atribuciones subsidiarias, por medio de la cooperación con diferentes órganos (Estado-Maior, 2017).

De acuerdo con esta interpretación y considerando también que el sistema propuesto poseerá capacidad dual, la Fuerza Terrestre podrá emplear sus capacidades de defensa de la patria para también cooperar con las agencias u órganos responsables de la seguridad pública, ofreciéndoles la oportunidad de integración de esfuerzos en beneficio del cumplimiento de las atribuciones específicas de cada uno de esos órganos, conforme a lo preconizado en el artículo 144 de la Constitución Federal (Estado-Maior, 2017).

La primera fase del SISFRON fue la implantación de un proyecto piloto, para el cual fue elegida la franja de frontera bajo responsabilidad de la 4ª Brigada de Caballería Mecanizada (4ª Bda C Mec), con aproximadamente 650 km de extensión, en la franja de la localidad de Mundo Novo-MS a Bela Vista-MS. (Silveira, 2017)

Pasados cerca de seis años del inicio del proyecto piloto, es posible verificar la evolución de las capacidades adquiridas por la 4ª Bda C Mec, entre los que destacan el incremento de la protección integrada[4], a través de recursos humanos capacitados

Fotografía: http://www.eb.mil.br/

[4] La protección integrada se concibe como la capacidad de proteger a la sociedad, realizando la garantía de los Poderes Constitucionales, la Garantía de la Ley y de la Orden, la protección de Estructuras Estraté¬gicas, la prevención y el combate a las acciones terroristas y la par¬ticipación de la Fuerza Terrenal en acciones en la franja de frontera, amplia colaboración del sector de seguridad pública (Estado-Maior, 2015).

y empleo de medios de vigilancia y de percepción, con la finalidad de proteger a la sociedad y estructuras estratégicas, de forma conjunta e interagencial.

Así mismo, esa capacidad sigue como un gran desafío, pues la operación de equipos de alta tecnología requiere tiempo para aprendizaje y operación, y retener recursos humanos en el mediano y largo plazo, lo cual requerirá cambios en el ciclo de instrucción, así como atractivos para mantener cuadros profesionales adiestrados en la franja de frontera.

La sensación de protección a la sociedad puede ser percibida con mayor evidencia durante las Operaciones Ágatas[5] más recientes, donde hubo aumento de la efectividad en la represión al contrabando, tráfico de drogas, crímenes ambientales, entre otras actividades ilícitas. Entre las atribuciones subsidiarias[6], la ejecución de obras de infraestructura y telecomunicaciones en Organizaciones Militares, así como la adquisición de equipos de alta tecnología impulsó a la industria nacional de defensa, generando empleo y renta y ampliando así la capacidad de apoyo a organismos gubernamentales.

Se han desarrollado capacidades de planificación y conducción, digitalización del espacio de batalla y sistemas de comunicaciones en conjunto con empresas asociadas, teniendo como órgano operacional local el Centro Regional de Monitoreo (CRM), en apoyo al Mando Militar del Oeste (CMO) que se refiere al análisis técnico de datos, operación de recursos de detección, soporte a la planificación de las misiones, realización de las actividades de Inteligencia de Señales y ejecución de la gestión logística de los medios asignados en su área de responsabilidad (Barbosa, 2014).

"LA ADOPCIÓN DE UN SISTEMA DE MONITOREO, DETECCIÓN Y APOYO A LA DECISIÓN EN LA FRANJA DE FRONTERA PERMITIRÁ A LA FUERZA TERRESTRE **POTENCIAR LAS ACTUALES CAPACIDADES** OPERATIVAS DE LAS TROPAS YA INSTALADAS O EMPLEADAS EN ESA FRANJA DEL TERRITORIO NACIONAL, YA SEA EN EL **CUMPLIMIENTO DE SU MISIÓN CONSTITUCIONAL,** ASÍ COMO ACTUANDO EN ATRIBUCIONES SUBSIDIARIAS, POR MEDIO DE LA COOPERACIÓN CON DIFERENTES ÓRGANOS."

[5] Operación Conjunta de las Fuerzas Armadas Brasileñas en coordina¬ción con otros órganos federales y estatales en la franja de frontera de la Amazonía para combatir delitos transfronterizos y ambientales.

[6] Ser capaz de cooperar para el desarrollo nacional y el bienestar social y para el apoyo al desarrollo económico y de infraestructura (Estado-Maior, 2015).

La estructura es complementada por la actuación de Centros de Operaciones, desde el nivel Batallón que, a través de la red, fija y móvil, de comunicaciones tácticas y estratégicas, poseen la capacidad de transmisión de datos en tiempo real.

Además, la obtención de información fue ampliada por la implantación de sensores de exploración del espectro electromagnético, radares de vigilancia, equipos de visión nocturna y termal, lo que potenció la conciencia situacional y mejor gestión del conocimiento e informaciones, elevando la capacidad de Comando y Control.

El apoyo logístico para las tropas desplegadas fue provisto por la implantación de nuevas estructuras organizativas como el Centro de Monitoreo de Fronteras, órgano central del SISFRON (Brasilia-DF), que tiene entre sus responsabilidades realizar la gestión logística del sistema, su modernización y coordinación de la gestión capacitación y simulación. El Proyecto aún tiene énfasis en el mantenimiento móvil, empleando equipos calificados para realizar mantenimiento preventivo y correctivo en todos los escalones, incluyendo la utilización de empresas que, mediante contratos tercerizados, podrán prestar el apoyo logístico al pleno funcionamiento del Sistema. (Barbosa, 2014)

Barbosa (2014, pág. 80) además complementa que la logística también involucra parte de la infraestructura del SISFRON, principalmente en lo que se refiere a las necesidades técnicas, operativas y administrativas, como por ejemplo la especificación de instalaciones; estructuras de soporte para radares fijos; redes de energía eléctrica, agua y alcantarillado; especificación de áreas climatizadas (servidores); entre otras, generando así la necesaria sustentación logística.

En cuanto a la interoperabilidad Conjunta e Interagencial, se ve que la Fuerza Terrestre podrá cooperar en la identificación de las amenazas transnacionales, por el suministro de las informaciones levantadas, para que los demás órganos gubernamentales actúen dentro de sus respectivas atribuciones. Esta cooperación, normalmente en situación de no guerra, se inserta en el contexto de Operaciones de Cooperación y Coordinación con Agencias, pudiendo el Sistema agregar medios que permitan la interfaz y la integración interagencial (Estado-Maior, 2017).

Fotografía: http://www.eb.mil.br/

> *"En cuanto a la interoperabilidad Conjunta e Interagencial, se ve que la Fuerza Terrestre podrá cooperar en la identificación de las amenazas transnacionales, por el suministro de las informaciones levantadas, para que los demás órganos gubernamentales actúen dentro de sus respectivas atribuciones."*

En el caso específico del SISFRON, aunque su estudio de viabilidad y alcance prevean la integración y la interoperabilidad con los sistemas de las demás fuerzas armadas y los Órganos de Seguridad Pública y de Fiscalización (OSPF), estas no fueron técnicamente contempladas en el proyecto básico, por lo que en el proyecto piloto se evidenció, en niveles superiores, una falta de definición de estándares mínimos de interoperabilidad organizacional (Silveira, 2017).

Esta deficiencia en la operación de sistemas comunes o compatibles, en particular en los medios de comunicación, genera una capacidad limitada de interoperabilidad.

En cuanto a la superioridad de las informaciones, el SISFRON posee ya estructuras instaladas de Guerra Electrónica e Inteligencia, como el 9º Batallón de Comunicaciones y Guerra Electrónica, el 6º Batallón de Inteligencia Militar y el CRM, que, sumadas a las capacidades de monitoreo de las tropas desdobladas de la franja de frontera, otorgan la ventaja operativa para la recolección, procesamiento, diseminación, explotación y protección de un flujo ininterrumpido de informaciones a los comandantes en todos los niveles, al mismo tiempo que busca sacar provecho de las informaciones del oponente y/o negarle esas habilidades (Estado-Maior, 2015).

De esta manera, se puede inferir que el SISFRON es un proyecto de alta complejidad y su desarrollo e implantación puede contribuir a mejoras doctrinales, organizativas (con la implantación de nuevas estructuras), de adiestramiento, materiales, educacionales, de personal e infraestructura, impactando positivamente la operatividad del Ejército brasileño.

CONCLUSIONES

Como se ha visto anteriormente, el SISFRON pretende potenciar la acción del Estado en la franja de frontera terrestre, ampliando la presencia y la capacidad de operación de los órganos gubernamentales, entre ellos el Ejército brasileño.

A pesar de la complejidad del proyecto, se superaron diversos desafíos para la certificación, como la logística y la integración de sensores y sistemas de comunicación. También cabe recordar que la implantación de un proyecto tan ambicioso en la franja de frontera ha sido obstaculizada por una serie de factores, como la escasez de recursos e infraestructura y la complejidad fisiográfica brasileña.

Sin embargo, a pesar de dichas dificultades, el proyecto piloto permitió certificar la eficiencia operacional del personal y medios empleados, sirviendo de laboratorio para la expansión del proyecto en las franjas de frontera adyacentes. De igual forma, indujo en diferentes grados las capacidades militares terrestres de apoyo a órganos gubernamentales, de Comando y Control, de sustentación logística, interoperabilidad y superioridad de las informaciones, lo cual ha sido una contribución excepcional para el Ejército brasileño en la era del conocimiento.

Por último, se puede afirmar que la implementación del Proyecto SISFRON fue una solución viable y factible para que Brasil incrementara la presencia estatal en la franja de frontera, ejerciendo la soberanía de manera más eficaz y ampliando la seguridad de la sociedad.

Fotografía: http://www.eb.mil.br/

BIBLIOGRAFÍA

Barbosa, C. G. (2014). O Sistema Integrado de Monitoramento de Fronteiras (SISFRON) frente às vulnerabilidades brasileiras e seus reflexos na cooperação regional. Rio de Janeiro, RJ, Brasil: Escola de Comando e Estado-Maior do Exército.

CDIF. (2010). Comissão Permanente para o Desenvolvimento e a Integração da Faixa de Fronteira. Fonte: http://cdif-cdif.blogspot.com/:http://cdif.blogspot.com/2012/11/cidades-gemeas-municipioscodigo-ibge.html

Constituição. (1988). Constituição da República Federativa do Brasil. Brasília: Diário Oficial da União. EPEx. (10 de Dez de 2015). Escritório de Projetos do Exército Brasileiro. Fonte: http://www.epex.eb.mil.br/index.php/imagens/category/22-16112015

EPEx. (2018). Palestra pt2 - Portfólio Estratégico do Exército. Brasília, DF, Brasil. Fonte: http://www.epex.eb.mil.br/images/pdf/EPEX_-Palestra_Pt2.pdf

EPEx. (2018). Portfólio Estratégico do Exército. Brasília, DF, Brasil: Estado-Maior. Escritório de Projetos do Exército. Brasil. Exército. (2019). Fonte: Exército Brasileiro: http://www.eb.mil.br/operacao-agata

Estado-Maior. (2013). Bases para a Transformação da Doutrina Militar Terrestre. Brasília: Exército Brasileiro.

Estado-Maior. (2015). Catálogo de capacidades do Exército. Brasília: Exército Brasileiro.

Exército. Estado-Maior. (21 de Nov de 2017). Portaria nº 462 - EME, de 21 de novembro de 2017. Aprova a Compreensão das Operações (COMOP) nº 08/2017, do Sistema Integrado de Monitoramento de Fronteiras (SISFRON). Brasília, DF.

Ministério da Defesa. (2017). Cenários de Defesa 2020 – 2039 – sumário executivo. Ministério da Defesa, Assessoria Especial de Planejamento. Brasília. Brasília: Ministério da Defesa. Acesso em 18 de 01 de 2019, disponível em https://www.defesa.gov.br/arquivos/estado_e_defesa/revista/revista_cenario_de_defesa.pdf

Ministério da Defesa. END. (2012). Estratégia Nacional de Defesa. Brasília, DF, Ministério da Defesa. Acesso em 18 de 01 de 2019, disponível em https://www.defesa.gov.br/arquivos/estado_e_defesa/END-PND_Optimized.pdf

Ministério da Defesa. PND. (2012). Política Nacional de Defesa. Brasília, DF, Brasil: Ministério da Defesa. Acesso em 18 de 01 de 2019, disponível em https://www.defesa.gov.br/arquivos/estado_e_defesa/END-PND_Optimized.pdf

Gabinete de Segurança Institucional. (2018). http://gsi.gov.br/. Fonte: Gabinete de Segurança

Institucional da Presidência da República do Brasil: http://gsi.gov.br/arquivos/ppif.pdf

Silveira, R. B. (2017). O SISFRON e as fronteiras: cenários prospectivos de integração sistêmica e interoperabilidade interagências. Rio de Janeiro, RJ, Brasil: Escola de Comando e Estado-Maior do Exército.

CAPABILITY BASED PLANNING. A FLEXIBLE APPROACH FOR A COMPLEX AND CHANGING ENVIRONMENT[1]

Institute for Defense Analyses

IDA is a not-for-profit research and development center funded primarily by the United States government. IDA's mission is to provide objective analyses of national security issues and related national challenges, particularly those requiring extraordinary scientific, technical, and analytic expertise.

RESUMEN

Capability Based Planning (CBP) is a force planning process that analyzes a broad range of threats and challenges. It is part of a process that ultimately seeks to align defense budgets to defense policy. Developing armed forces through CBP creates a future force optimized toward tackling a large number of prioritized threats instead of a small number of specific threats. Capability is the product of a set of well-integrated components (e.g., personnel, training, equipment, and facilities). There are prerequisites to CBP. These include an accepted definition of capability and its components, an empowered senior leader who has a dedicated planning staff with analytic capability, a joint planning culture, strategic policy guidance, planning scenarios, operating concepts responsive to scenarios, a risk assessment framework, and a capability taxonomy or partition. A taxonomy or partition is a hierarchy that describes and categorizes the capabilities within a force structure and allows analysts to match capabilities with the units of the armed forces' structure. Nations beginning to implement CBP will often run into year zero problems due to their lack of the prerequisites. IDA proposes a three-phase CBP process, the first of which directly addresses the development of the CBP prerequisites.

[1] This manuscript was authored by Research Staff Members from the Institute for Defense Analyses' (IDA) Studies and Analyses Center, Alexandria, Virginia.

Palabras clave: *CBP, taxonomy, optimization, strategic policy, risk, structure.*

PLANEACIÓN BASADA EN CAPACIDADES: UNA APROXIMACIÓN FLEXIBLE A UN AMBIENTE COMPLEJO Y CAMBIANTE

RESUMEN

La planificación basada en capacidades (PBC) es un proceso de planificación de la Fuerza que analiza una amplia gama de amenazas y desafíos. Es parte de un proceso que busca alinear los presupuestos de defensa con la política de defensa. El desarrollo de las fuerzas armadas, a través de la PBC, crea una fuerza futura optimizada para enfrentar una gran cantidad de amenazas elevadas, en lugar de una pequeña cantidad de amenazas específicas. La capacidad es el producto de un conjunto de componentes bien integrados (por ejemplo, personal, capacitación, equipo e instalaciones). Hay requisitos previos para la PBC. Estos incluyen una definición aceptada de capacidad y sus componentes, un líder senior con poder que cuente con un personal de planificación, con capacidad analítica; una cultura de planificación conjunta; orientación de políticas estratégicas; escenarios de planificación; conceptos operativos; un marco de evaluación de riesgos y una Capacidad de taxonomía o partición. Una taxonomía o partición es una jerarquía que describe y clasifica las capacidades dentro de una estructura de fuerza y permite a los analistas relacionar las capacidades con las unidades de la estructura de las fuerzas armadas. Las naciones que comienzan a implementar la PBC a menudo se encontrarán con problemas desde el año cero debido a su falta de requisitos previos. El Institute for Defense Analyses (IDA) propone un proceso de PBC basado en tres fases. La primera de ellas aborda directamente el desarrollo de los requisitos previos de la PBC.

Palabras claves: *PBC, taxonomía, optimización, política estratégica, riesgo, estructura.*

INTRODUCCIÓN

The past three decades have been a time of constant and rapid change. The dissolution of 20th century norms of international relations and significant technological transformation disrupted global social, political, environmental and economic conditions, which created new, asymmetric security challenges for governments.

Resultantly, armed forces are now expected to respond to multiple and diverse challenges—sometimes simultaneously. While fighting wars against an armed enemy is still a role of military services, they are now utilized just as much if not more for peacekeeping, disaster response, fighting heavily armed transnational organizations, combatting violent extremist groups or managing borders during mass migration events. These demands stress armed forces primarily designed to deter, respond to, or engage the armed enemies of the state.

As challenges increase, citizens demand more versatility from their military. However, given the lack of a singular, unifying threat to national sovereignty there has also been an inconsistent yet simultaneous desire to reduce the armed forces' budget. So, even as the security challenges confronting armed forces became more diverse, the challenge of justifying and defending the defense budget became more difficult. Given these dynamics, defense ministries and armed forces turned to capability-based planning (CBP). CBP is a process to determine an efficient and effective armed forces structure, and to provide logic and evidence in support of defense budget requests.

The most widely cited definition of CBP is from Paul Davis of the RAND Corporation. Davis (2002) wrote that CBP, "is planning, under uncertainty, to provide capabilities suitable for a wide range of modern-day challenges and circumstances while working within an economic framework that necessitates choice." The objective of CBP is to develop a flexible, robust, and adaptable force structure that is also manageable and affordable.

"CBP is a process to determine an efficient and effective armed forces structure, and to provide logic and evidence in support of defense budget requests."

Davis (2014) explains that "[when] done well…capabilities-based planning confronts uncertainty and the need to make choices within constrained budgets. Properly understood, it has always considered both generic possibilities and specific threats." The consideration of generic possibilities differentiates CBP from threat-based planning. Threat-based planning is useful when threats are easily recognized and can be described by one or a few reasonable scenarios. CBP is more useful when threats and challenges are multi-faceted and uncertain.

CAPABILITY. UNDERSTANDING THE TERM

The focus of CBP is to generate a force development plan, which, through directed actions and the allocation of resources, creates armed forces that can fulfill objectives assigned to the defense sector. Nations that use CBP include but are not limited to Australia, Canada, The Philippines, The United States, and The United Kingdom. Among the nations that use CBP, there are three common elements in each nation's definition of capability.

First is the idea of wherewithal to complete a task or produce an effect. Second, each definition describes capability as the means to overcome temporal and physical constraints in order to complete a task or produce an effect. Third, each definition refers to a performance standard. All three elements are important because capability is "only a meaningful concept for defense planning when it is specific about whose capability, to do what, and under what circumstances." (Yue & Henchaw, 2009). This means that capability is dependent on the context and capacity – capacity being the amount of capability. To synthesize these three elements, we propose that *capability is the wherewithal to complete a task or produce an effect within a set of specified performance standards and environmental conditions.*

In order to plan a force structure based on capability, it is necessary to understand how to create capability. In other words, what is capability comprised of and how is capability created within armed forces units so they can complete tasks and produce effects to a specific performance standard. To explain, we describe capability as having components. When the components are properly integrated across the units of a force, it is capable. These components (for example, doctrine, personnel, training, facilities and equipment[2]) provide a means for defense planners to analyze the sufficiency (or capacity) and effectiveness of a unit's capability.

"THE FOCUS OF **CBP IS TO GENERATE A FORCE DEVELOPMENT PLAN,** WHICH, THROUGH DIRECTED ACTIONS AND THE **ALLOCATION OF RESOURCES,** CREATES ARMED FORCES THAT CAN FULFILL **OBJECTIVES ASSIGNED TO THE DEFENSE SECTOR."**

[2] For the United States Armed Forces the components are DOTMLPF. Doctrine, Organization, Training, Materiel and Equipment, Leadership and Education, Personnel, and Facilities.

Fotografía:Ejército Nacional de Colombia

CPB AND THE OVERALL SYSTEM OF DEFENSE MANAGEMENT

CBP is focused on developing the future force, not leading or employing the current force. Force development processes should aim to inform senior leader decision making on how to organize, train, equip, and resource future armed forces so they are capable of dealing with the nation's security challenges within the budget limit allocated to the armed forces. Once capable units have been provided to the military services, their commanders must prepare the forces to be employed.

Force development and force employment flow from defense policy and strategy, but their view of the future is different. Force development is forward looking. It entails planning to invest in and build the future force structure through defense resource management, human resource management, and logistics. Modifying an existing force structure takes time; thus, force development processes focus beyond the time period considered by ongoing operational planning. Force employment is focused on the near term. It is planning and then preparation (through training and exercises) to use the existing force to accomplish objectives within the near future. Figure 1 illustrates the different processes and relationships of force development and force employment.

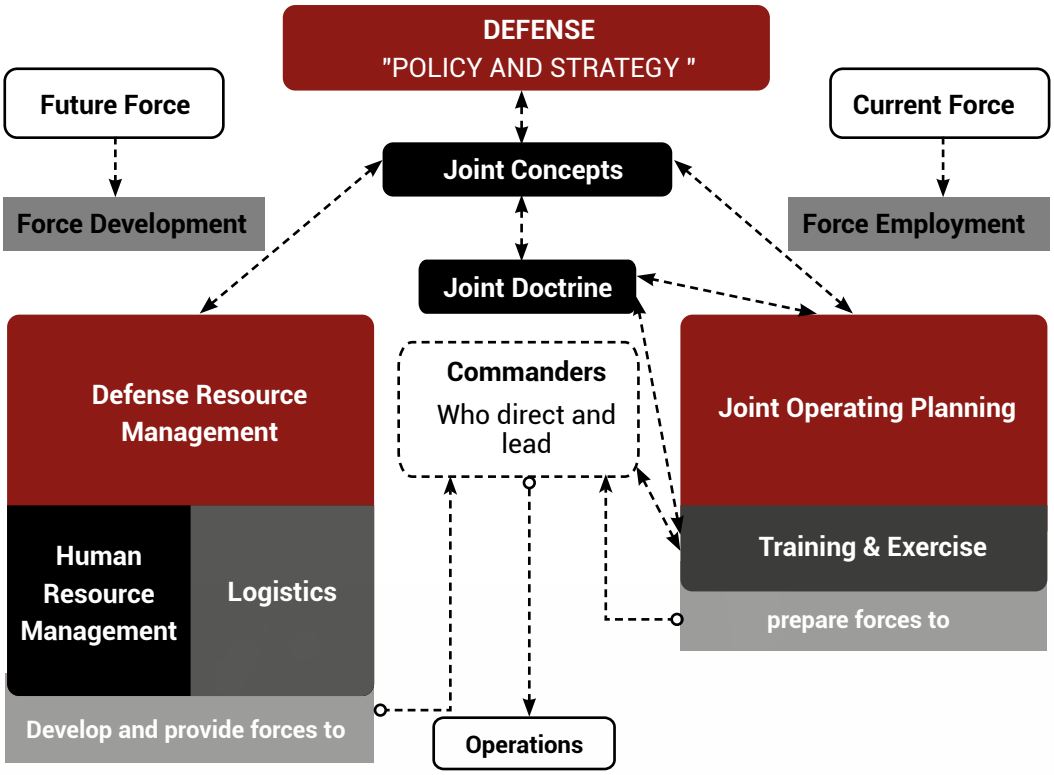


Figure 1. Defense Management Processes Relate to Force Development and Force Employment

Fotografía:Ejército Nacional de Colombia

CBP focuses on force development, and it is one of four Defense Resource Management Processes (the other three being program planning, acquisition planning, and budget planning). To reiterate, CBP focuses on force development. It is not a process to correct operational deficiencies in today's force. That is a job for the commanders and the leaders of units who must utilize operational art[3] to maximize the effectiveness of their units.

CBP's goal is to produce a future force able to deal with the challenges of the future. How far into the future is subject to a choice of defense leadership. If near-term problems abound, then leadership may focus CBP to correct gaps in capability as soon as possible. If the near future appears secure, then leadership may assess the current force against a longer term planning horizon.

Defense resource management processes connect defense policy to budget execution. Collectively, capability planning, program planning, and budget planning direct how defense resources (money, personnel, equipment, facilities, and so forth) are allocated to produce capability. These planning processes are interrelated, like gears in a machine. They drive and provide feedback to one another. Figure 2 is a force development model. It illustrates how defense resource management's planning processes link policy to budget execution.

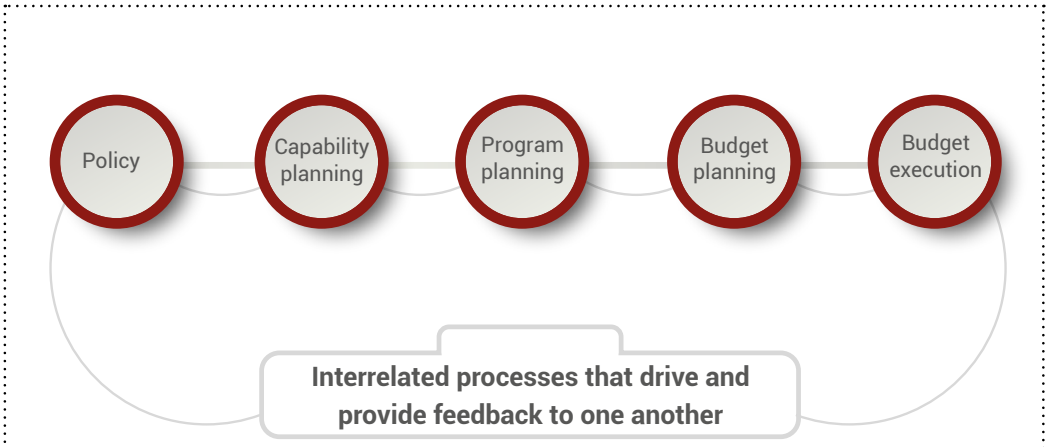


Figure 2. **Force Development – Planning Links Policy to Budget Execution**


Fotografía: Escuela de suboficiales (EMSUB) Ejército Nacional de Colombia

[3] Operational art is "the cognitive approach by commanders and staffs—supported by their skill, knowledge, experience, creativity, and judgment—to develop strategies, campaigns, and operations to organize and employ military forces …" (The Pentagon, 2018).


Fotografía:Ejército Nacional de Colombia

A defense minister's policy provides guidance for the development of the force. In response to that guidance, CBP determines the means necessary to achieve the minister's guidance. Program and budget planning allocate resources to develop the capabilities over a multi-year period. Finally, the budget is executed to pay for capability components that are allocated to units.

PREREQUISITES FOR CBP

The first two prerequisites for CBP, which have already been discussed, are an approved definition of defense capability and an agreement on what the components of capability are. However, there are other necessary prerequisites for using CBP.

Senior leadership of the CBP process

Authority to oversee the process and empowered to make decisions must reside at a senior level in the defense sector; either within the Defense Ministry or the Chief of Defense staff. CBP may result in short-term losses for some stakeholders within the defense sector. A consensus approach to planning does not allow for such losses. Further, consensus is a poor method for planning a capable force within a budget constraint. So, a senior leader needs to be empowered and accountable for investigating options, providing advice to the government about difficult decisions, and to propose and make decisions that may harm a specific stakeholders' short-term interest in the long-term interest of national security.

A joint planning perspective

Individual military services have a natural bias to favor their own perspective and that bias often favors new equipment purchases. CBP relies on a joint perspective in order to provide the best mix of capability at an affordable price for a nation. Planning should produce capability to achieve the strategic objectives of the government—not to satisfy the needs of a particular military service. Individual services may have unique capabilities, but whether or not they are necessary or add value must be analyzed from a joint perspective.

A dedicated planning staff with analytic capability

CBP needs a dedicated organization that leads a joint planning process to identify capability gaps and conduct sector-wide tradeoff analyses across all warfighting and enterprise (support) functions to determine how to close gaps. This means a staff of subject matter experts who have the right knowledge and experience.

Defense policy guidance

Guidance directs and bounds the capability planning process. A good planner should be able to plan for anything he or she must is directed to consider; however, no one can plan for everything. Therefore, defense policy guidance should prioritize the armed forces mission areas and security challenges and provide guidance on what risks to national security are undesirable vs. unacceptable.

Scenarios

CBP's intent is to design a force that can contend with a broad range of challenges and associated contingencies. Force planners need scenarios that describe how future challenges may present themselves. Further, each scenario needs defined success criteria that help the armed forces conceptualize a response. Success criteria are used to determine the way to respond and the means necessary to respond to a scenario's challenges.

Concepts

Concepts describe how the armed forces may operate given a future operating environment and its challenges. A concept ways capabilities will be used to achieve an objective in a specified operating environment or against specified challenges (Ween, 2013). In this way, concepts link the ways the Armed Forces will accomplish its objectives to the ends specified in defense policy guidance and to the means the defense resource management process produces.

"IF ALL PREREQUISITES OF CBP ARE PRESENT, THEN A FORCE DEVELOPMENT **STRATEGY IN RESPONSE TO POLICY GUIDANCE** CAN EMERGE AND PROVIDE A VISION OF HOW TO **DESIGN THE ARMED FORCES OF THE FUTURE.** IN OTHER WORDS, THE INTEGRATION OF THESE PREREQUISITES INTO A COHERENT APPROACH TO FORCE DEVELOPMENT IS A FORCE **DEVELOPMENT STRATEGY."**


Fotografía:Ejército Nacional de Colombia

Risk assessment

Scenarios describe the potential security challenges a nation may face within a given mission area. Implied within the challenges are risks. Defining which risks are tolerable, acceptable, unbearable, or otherwise is a policy decision. However, planners need a way to assess and describe risk so policy makers can decide whether the identified risk is acceptable or unacceptable. Risk assessment allows the planning staff to make informed tradeoffs as they work to identify what capabilities should be developed given finite resources.

Capability taxonomy

A capability taxonomy is a framework that decomposes all defense capabilities into a defined hierarchy. All nations that use CBP must have a joint capability taxonomy with the following four characteristics.

1. Exhaustive: The taxonomy needs to document the capability of the entire force structure.
2. Mutually Exclusive: A capability can only appear in the taxonomy one time.
3. Distinctive: Every capability in the taxonomy must be unique from any other
4. Living: A taxonomy must be able to change. The world is not static. A process to manage and update the taxonomy over time is required.

If all prerequisites of CBP are present, then a force development strategy in response to policy guidance can emerge and provide a vision of how to design the armed forces of the future. In other words, the integration of these prerequisites into a coherent approach to force development is a force development strategy.

THE CBP PROCESS

Essentially, CBP is a two-step analytic process. The first step considers whether the units across the joint force are able to perform tasks and produce effects under a specified set of standards and conditions. If this is true, then the force is capable enough. If not, then a capability gap exists. The second step considers how to close or mitigate capability gaps within the parameters provided by defense policy guidance and known fiscal restraints.

Capability requirements are derived from analyses of policy guidance, scenarios, and concepts. Comparing a unit's capability to its requirements uncovers potential gaps. Gaps are mitigated or closed by considering how to rearrange, increase, or decrease the components of capability (e.g., DOTMLPF) within units. Figure 3 illustrates this idea. Units (or force elements as depicted in figure 3) are the focus of analyses.

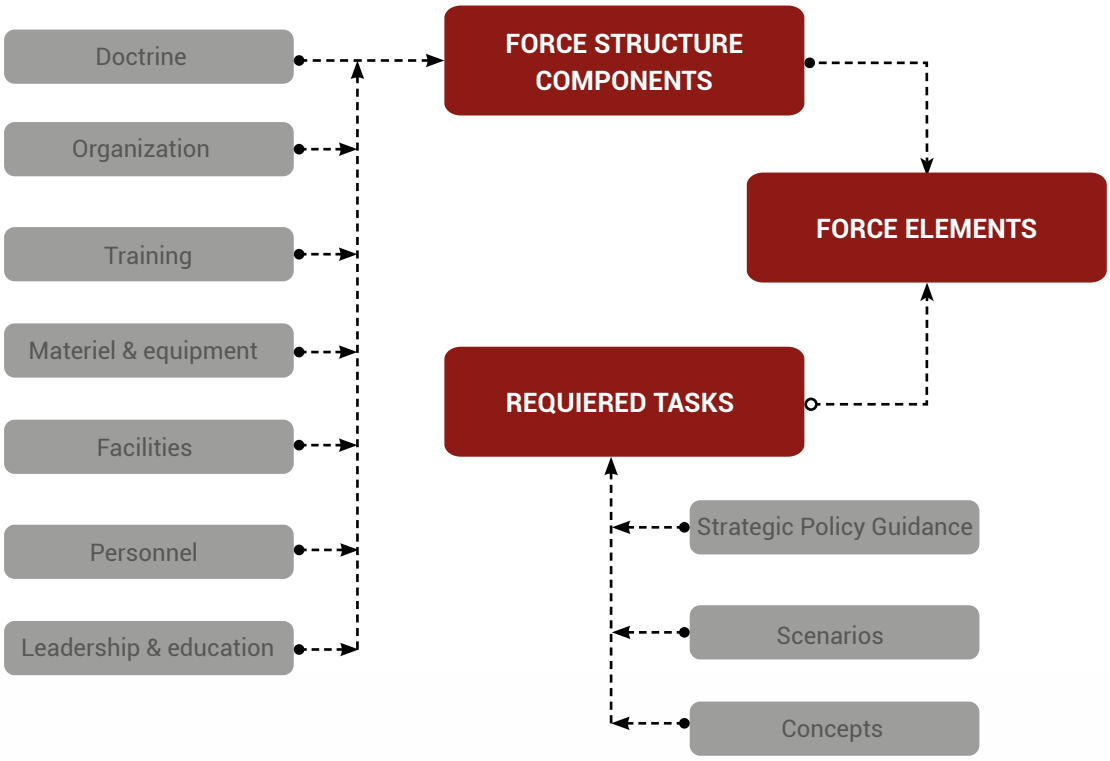


Figure 3. **Capability Planning: Force Elements Are the Focus of Analyses**

Capability planning completes both analytic steps through a deliberate process. Given IDA's experience in helping nations develop a CBP process, we recommend the three-phase approach depicted in Figure 4. This approach is mindful that a nation may not have all the prerequisites for CBP in place before it tries to implement CBP.

Fotografía:Ejército Nacional de Colombia

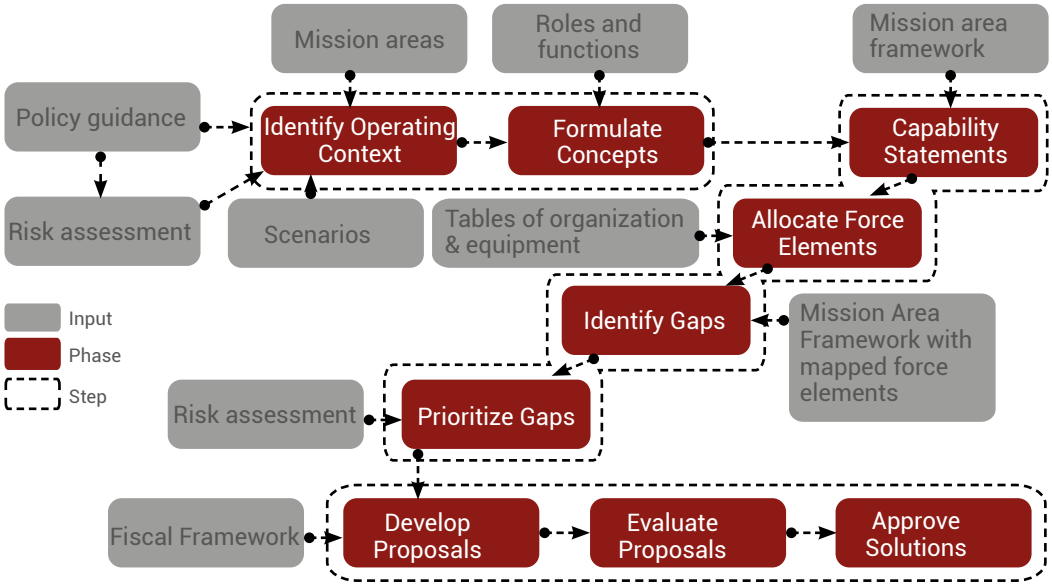


Figure 4. **IDA's Recommended CBP Process**

Phase 1. Derived from scenarios and policy guidance and informed by risk assessment, step one identifies the operational context and the challenges it will present to effective operations. Step two develops concepts that satisfy the success criteria in the scenarios given. Any other policy guidance that obligates or restricts armed forces' actions must also be considered. This phase tackles year zero problems head-on by ensuring that the CBP prerequisites of defense policy guidance, scenarios, risk assessment, and concepts are developed. If a nation has already developed all the prerequisites, this phase will be short since it only gathers up work that has already been done.

Phase 2. For each scenario and its corresponding concept or set of concepts, phase 2 identifies capabilities required to implement each concept. Then, existing force elements (i.e. units) are allocated to each capability, and the force structure is analyzed to identify gaps. Finally, the gaps are prioritized and provided to the Defense Minister or Chief of Defense for approval.

Phase 3. The purpose is to evaluate and analyze the prioritized capability gaps approved at the end of phase 2 and to develop solutions to close or mitigate those gaps. Approved solutions, depending on their nature, may be referred to the defense budget or acquisition process. Alternately, the solution may require the armed forces to develop new doctrine or to reorganize. Complex solutions may require all the above.

FINAL THOUGHTS

The emergence of joint perspectives in capability planning have increased over the last twenty years. This trend is seen not only in NATO nations like the UK and Canada, but also in nations such as Colombia and the Philippines. The transition away from force planning led by individual military services is not easy. It requires substantial investments in time and effort, and demands senior leader commitment and involvement.

Capability planning's greatest contribution is to align Defense Resource management processes more closely to the joint operations of their Armed Forces. Gone are the days in most countries where independent services operate solely in their own domains. Today, most Armed Forces recognize the value and contribution of joint operations; a nation's force development process should do the same.

Fotografía:Ejército Nacional de Colombia

BIBLIOGRAFÍA

Davis, P. (2014). *Analysis to Inform Defense Planning Despite Austerity*. Obtenido de Rand Corporation: https://www.rand.org/pubs/research_reports/RR482.html

Yue, Y. Henshaw, P. (2009). *A Holistic View of UK Military Capability Development," Defense and Security Analysis, 25, no. 1* . Obtenido de https://www.tandfonline.com/doi/pdf/10.1080/14751790902749900?needAccess=true.

The Pentagon. (November de 2018). *DOD Dictionary of Military and Associated Terms*. Obtenido de http://www.jcs.mil/Portals/ 36/Documents/Doctrine/pubs/dictionary.pdf

Ween, A. (2013). *Analysis of Whole-of-Force Design and Planning*. Obtenido de Defense Science and Technology Organization, Joint and Operations Analysis Division: http://ismor.cds.cranfield.ac.uk/30th-symposium-2013/analysis-of-whole-of-force-design-andplanning/@@ download/paper/30ismor_ween_paper.pdf.

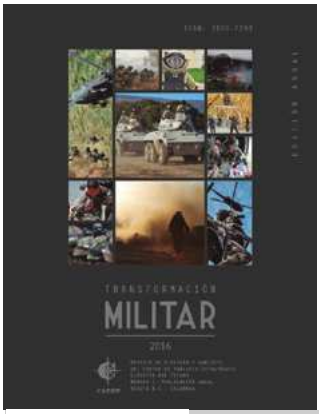
Davis, P. (2002). *Analytic Architecture for Capabilities-Based Planning, Mission-System Analysis, and Transformation*. Obtenido de Rand Corporation: https://www.rand.org/pubs/monograph_reports/MR1513.html.

Fotografía:Ejército Nacional de Colombia

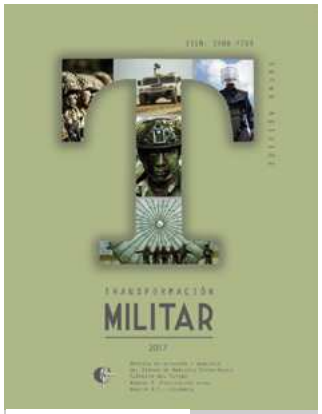
RTM 4

REVISTA TRANSFORMACIÓN MILITAR ED N°

PUBLICACIONES ANTERIORES



2016



2017

2018

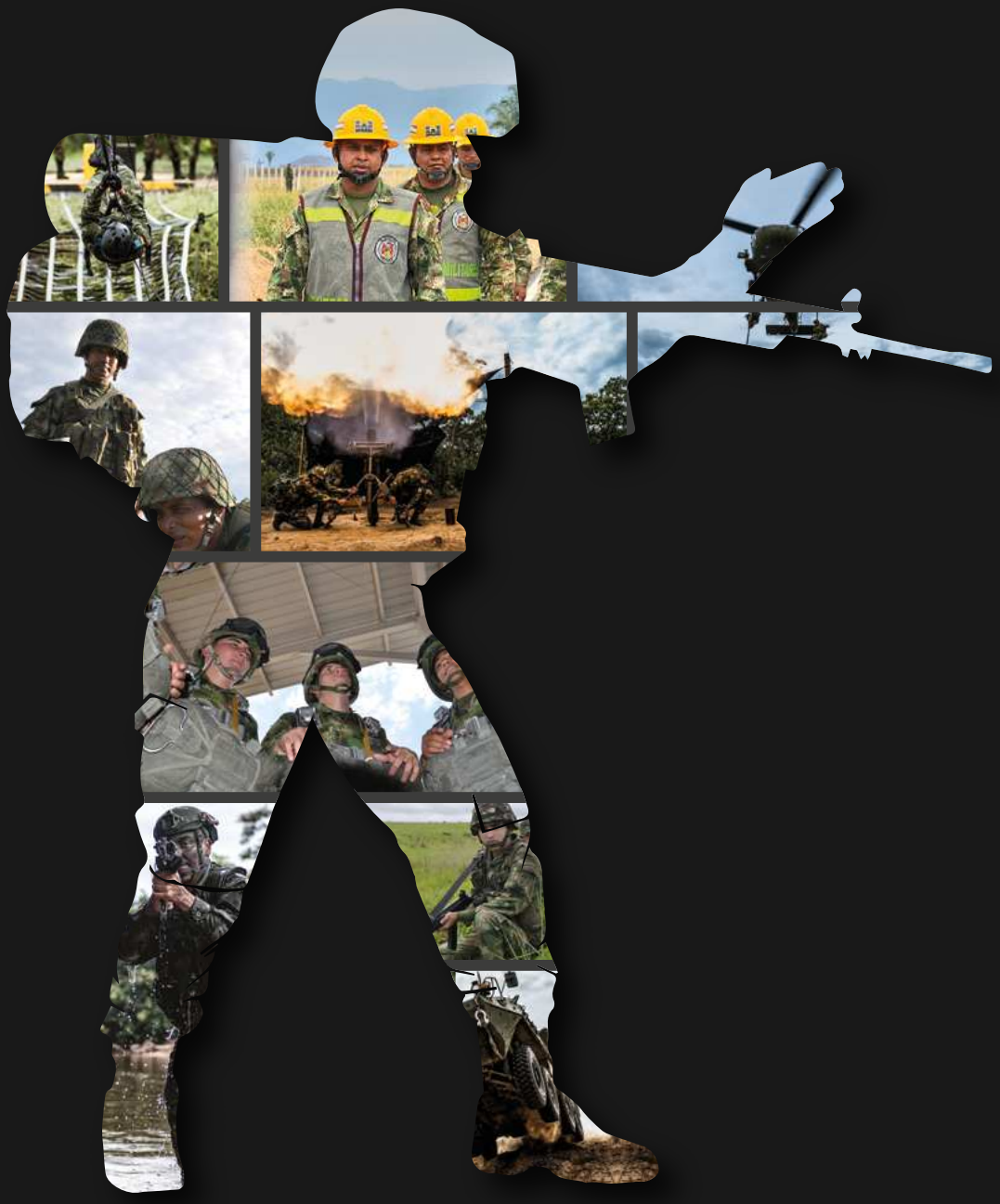
Escanea estos códigos para acceder a estas ediciones

2020 | FORTALECIMIENTO DE LA PROFESIONALIZACIÓN MILITAR Y COHESIÓN DE LA FUERZA

2020 / 04

TRANSFORMACIÓN MILITAR

EDICIÓN ANUAL



Ejército Nacional de Colombia

@COL_EJERCITO

centrodeanalisisestrategico@gmail.com

independent.academia.edu/Cotefcaeef