Formación militar en ciberdefensa:

Apreciaciones exploratorias sobre Brasil, Chile y Colombia

Por Dr. Guillermo Rutz

Resumen: este artículo brinda aspectos exploratorios para la discusión de cuestiones específicas referidas a la formación militar en ciberdefensa, desde la perspectiva de las ciencias sociales, a partir de fuentes académicas, militares y diplomáticas de Brasil, Chile y Colombia. Las fuentes fueron entrevistadas durante el año 2021. El artículo se enmarca en el contexto del Proyecto UNDEFI "Paz y guerra en el ciberespacio: Formación militar en ciberdefensa" de la Facultad de la Defensa Nacional. Realiza un recorrido por los antecedentes de la producción académica correspondientes a los países mencionados. Aborda, desde la perspectiva de las fuentes entrevistadas, esas experiencias nacionales y sus miradas estratégicas y geopolíticas. Asimismo, indaga la formación de los Recursos Humanos: perfiles, capacitación y reclutamiento para la ciberdefensa.

Palabras claves: ciberespacio, ciberdefensa, formación militar, estrategia y geopolítica, Latinoamérica

Introducción

La discusión y abordaje académico, al igual que los aportes desde las ciencias sociales, en el ámbito civil, de la ciberdefensa como tema de estudio, al menos en la producción científica actual de Argentina, no sólo amerita, sino que además demanda de registros escritos que den cuenta sobre la formación en el área. Sobre el particular, son muchos y diversos los enfoques que se le pueden dar a la investigación, la reflexión o artículos que se escriban; dependerán del interés personal del investigador, de la institución o el contexto académico, político y técnico en el cual se inserten dichos debates. Cuando se analizan cuestiones educativas, o de formación de una temática, surgen asuntos institucionales, políticas, estratégicas, curriculares, culturales, sociales, técnicas y científicas referidas al objeto de estudio. Claro que no siempre interesan, no siempre se condicen con la agenda del tema o no hay tiempo para profundizar al respecto. Es en este sentido, que el artículo presenta apreciaciones de carácter exploratorio, desde la perspectiva de las ciencias sociales, sobre la formación militar en ciberdefensa a partir de la experiencia y percepciones de fuentes diplomáticas, académicas y militares de tres países de la región: Brasil, Chile y Colombia. El artículo surge de la investigación llevada a cabo en el marco del Proyecto UNDEFI "Paz y guerra en el ciberespacio: formación militar en ciberdefensa", de la Facultad de la Defensa Nacional, en la Universidad de la Defensa, República Argentina, durante el primer semestre del año 2021.

El objeto de esta investigación estuvo puesto en conocer de forma exploratoria, la mirada estratégica y geopolítica, como también experiencia de los tres países mencionados, en cuanto a la formación militar de recursos humanos para la ciberdefensa. Para ello se indagó mediante entrevistas en profundidad sobre seis ejes vinculados a la temática: paz en el quinto dominio, pensar los Recursos Humanos, puestos por sector, perfiles profesionales, capacitación de los recurso humano y reclutamiento. Se incluye además un estado del arte de las publicaciones académicas más relevantes que abordan las temáticas de ciberdefensa, ciberespacio y ciberseguridad, cuyo origen de publicación corresponde a los países involucrados en el presente trabajo.

Antecedentes en la producción académica

En Brasil, Lopes (2014) reflexiona respecto del proceso de securitización desde el campo cibernético, en tanto que Rogers (2015) compara los enfoques de Estados Unidos y Brasil sobre el manejo y gestión de la información de inteligencia para la seguridad multilateral del ciberespacio. A su vez, Lopes Carneiro (2016) se refiere a la defensa cibernética como extensión del rol constitucional que tienen las fuerzas armadas. Por último, Di Beneditto (2017) escribe sobre la ciberdefensa y seguridad para los sistemas ciberfísicos de los medios operativos de superficie.

En el caso de Chile, Balmaceda Hoyos (2011) escribe acerca del delito de estafa informática y Polloni Contardo (2015) aborda el escenario que actualmente presenta el campo de la ciberseguridad. Sobre la Política de Ciberdefensa en el marco de la defensa nacional, Gómez Urrutia (2016) presenta la visión del Ministro de Defensa de Chile. A su vez, Sancho Hirane (2016) se refiere al Ciberespacio como bien público mundial y Gómez (2018), aborda diferentes cuestiones referidas a una defensa moderna, entre las cuales también menciona la Ciberdefensa.

Por otra parte, Sancho Hirane (2018 a) escribe sobre Ciberseguridad y política públicas, mientras que Aranda Mora (2018) se ocupa de ciberseguridad y ciberdefensa y, para ello compara ataques físicos y cibernéticos en función de lo cual luego define ciberseguridad y ciberdefensa. Al mismo tiempo, Álvarez Valenzuela, (2018) trabaja sobre ciberseguridad en América Latina y ciberdefensa en Chile, en tanto que Leiva (2018) plantea si la Ciberdefensa constituye un nuevo eje estratégico. En la producción científica de 2018 se puede incluir también a Martabit Tellechea (2018a) quien plantea que parte importante de la problemática del ciberterrorismo, recae en las dificultades descriptivas encontradas en el concepto terrorismo, que luego emigraron al ciberespacio; también sostiene, Martabit Tellechea (2018b), que en la búsqueda de seguridad en el ciberespacio, se presenta una dicotomía entre potenciar la libertad de los individuos y asegurar la red global contra amenazas reales y potenciales al Estado. Por otra parte, en relación al ciberespacio,

Sancho Hirane (2018b) aborda la noción de "ciberinteligencia" como término que emerge en el marco de la existencia de una nueva dimensión.

En el mismo ámbito chileno, Amigo Tossi (2019) sostiene que la ciberamenaza es uno de los principales riesgos para la seguridad de los países, en tanto que Witker Barra (2019) contribuye ocupándose del Ciberespacio e inteligencia artificial. Así mismo, Barria Huidobro (2019) sostiene que el ciberespacio ha cambiado tanto paradigmas tradicionales como modernos, desde las relaciones sociales y los negocios hasta los dominios de guerra, por ello considera que una defensa moderna requiere de una capacidad no solo técnica y tecnológica para abordar este espacio virtual y sus desafíos, sino también de una capacidad organizacional y administrativa. A su vez, Martabit Tellechea (2019a) trabaja el concepto de ciberespacio desde sus atribuciones y su relación con el Derecho Internacional; de igual modo, Martabit Tellechea (2019b), plantea que los asuntos de ciberseguridad hoy se encuentran en una fase de definición de normas y límites de acción en el derecho nacional e internacional. Más recientemente, Barria Huidobro (2020) aborda el caso de la cibergeografía como disciplina emergente vinculada al área; en tanto que Valdivia Cerda (2020) postula que en un escenario de alta complejidad y volatilidad los Estados observan el desarrollo de los asuntos espaciales como un fenómeno inédito, redundando en el incremento de los niveles de incertidumbre frente a un cambio de balanza de poder global, el artículo analiza la evolución de los asuntos espaciales y la necesidad de articular el enfoque de la metageopolítica, incluido lo ciber.

En Colombia, Sánchez-Bustamante (2013) daba cuenta de un nuevo campo de lucha al escribir sobre las fuerzas militares colombianas y su trabajo con socios regionales en el ambiente ciber. Un año después Niño Wilches (2014) explica sobre el carácter de las amenazas (en el ciberespacio), el alcance de las ventajas y desventajas, las proyecciones y los ciberataques. En el mismo sentido, Pinedo Herrera (2015) expone las principales consideraciones tenidas en cuenta para el desarrollo de políticas públicas relacionadas con ciberseguridad, destinadas a procurar una ciberdefensa enfocada a la prevención, detección y neutralización de amenazas informáticas. Por otra parte, Arias Torres y Celis Jutinico (2015) publican respecto a un modelo experimental de ciberseguridad y ciberdefensa para

Colombia; al mismo tiempo que Cortes Borrero (2015) da cuenta del avance en cuanto a la política pública de Ciberseguridad y Ciberdefensa en el país. A su vez, Sánchez-Lozano (2016) aborda la temática sobre los lineamientos de política en ciberseguridad y ciberdefensa y, Cáceres García (2017) lo hace respecto al tratamiento académico de una estrategia nacional en ciberseguridad y ciberdefensa.

Más recientemente en el tiempo, Pinto et al. (2018) se refiere a la Inteligencia de fuentes abierta (OSINT) para operaciones de ciberseguridad, y Marin et al. (2019) escribe sobre el Modelo Ontológico de Ciberdelitos. Luego Pinzón Bueno (2020) se refiere a la modernización y futuro de las fuerzas armadas y cómo atraviesa esta temática lo ciber, en tanto que Cujabante Villamil, et al. (2020), exploran el desarrollo institucional acerca del dominio del ciberespacio en Colombia y su incidencia sobre las relaciones cívico-militares en el país. Por otra parte Ospina y Sanabria (2020), analizan los desafíos nacionales frente a la ciberseguridad en el escenario global. También Realpe y Cano (2020) ponen en la agenda académica lo relativo a amenazas cibernéticas a la Seguridad y Defensa Nacional. Finalmente podemos mencionar que Laverde Castillo y Hernández Bejarano (2021) trabajan como temas la ciberseguridad, ciberdefensa, inteligencia, Estrategias de Seguridad Nacional y ciberespacio. Para ellos, las tecnologías, la información y los delitos, entre otros, sufrieron un gran cambio y evolución en los últimos años, lo cual presenta mayores desafíos y mayor grado de dificultad en su abordaje para la ciberdefensa y ciberseguridad.

Paz en el quinto dominio

En el caso de Brasil los expertos entrevistados, no pudieron dar cuenta de producciones académicas que traten directamente de la paz en el quinto dominio, si en cambio mencionan publicaciones que tratan de la guerra en este contexto. Respecto a la posición geopolítica del país sobre la paz en el quinto dominio, la posición diplomática brasileña es de solución pacífica de los conflictos, basada en la negociación. Este punto de vista también es aplicado en el dominio cibernético, en el cual la mayor atención del país (de acuerdo a los entrevistados) está puesta en el respeto a la privacidad de las personas (Ley General de Protección de Datos, Ley Carolina Dieckman), protección de las informaciones

del Estado y de la Sociedad Civil (Marco civil, Política Nacional de Seguridad de la Información) y la transparencia del Estado sobre el ciudadano (Ley de Acceso a la Información). Sin perjuicio de lo mencionado, Brasil identifica amenazas potenciales y reconoce la necesidad de fortalecer el campo cibernético de la Defensa lo cual se halla manifestado a través de la Estrategia Nacional de Defensa y el Libro Blanco de la Defensa. Desde la perspectiva de la Defensa, hay interés en el mantenimiento de la paz en este dominio, basando dicho interés en el daño potencial que puede causar a la Sociedad las acciones maliciosas en el espacio cibernético, en particular lo que pueda afectar la infraestructura crítica nacional. En este sentido, Brasil cree conveniente fortalecer la cooperación con los demás países de la región, aún más cuando se consideran las principales características del espacio cibernético, la ausencia de fronteras definidas, el largo alcance, la velocidad de las mudanzas y agilidad de acciones. Desde la perspectiva geopolítica y estratégica de Brasil, sólo se puede obtener la paz en el quinto dominio a través de acciones transparentes y basadas en la confianza mutua, lo que tarda en construirse en los ámbitos bilateral y multilateral; sin embargo, consideran que, en términos prácticos, todavía no es posible hablar de paz en el ciberespacio, ya que los crímenes cibernéticos pasan todos los días en todos los países del mundo.

Los especialistas chilenos consultados tampoco pudieron referenciar bibliografía nacional que trate sobre la paz en el ciberespacio, reconocen que se nutren académicamente de autores israelitas, norteamericanos, mexicanos, españoles, pero aquellos, en ningún caso hacen mención o abordan el tema de paz específicamente. Desde esta perspectiva, la paz en el quinto dominio está asociada a múltiples factores, donde lo fundamental es que tiene que haber disuasión de por medio. De acuerdo al enfoque mencionado los investigadores chilenos definen tres factores fundamentales: todo lo que es la información o el contexto de los datos, todo lo que es la sociedad en red desde la perspectiva de las redes sociales, todo lo que es el mercado desde el punto de vista financiero. A partir de esas tres variables estiman que quien tenga el control de las tres, va a tener el poder sobre el quinto dominio. De esta manera, su modelo postula que la paz en este espacio se logra, en parte a través de la disuasión, mostrando que es lo que se tiene, con qué cooperación internacional cuentan;

particularmente porque piensan que la ciberamenaza no tiene una característica física, siendo además un tema complejo de abordar. Y es por ello que incluyen a la cooperación internacional a través de los distintos tratados como un elemento clave, donde el más clásico es el tratado de Budapest para enfrentar la ciberdelincuencia y, los manuales de Talin como un claro reflejo de que la cooperación internacional y la ciberdisuasión frente a esta temática son la clave para poder hacerle frente a esta dimensión. En cuanto a la importancia estratégica que Chile le da al tema, ésta se vio impactada cuando el país comenzó a ser afectado por una serie de ataques informáticos que, en las propias voces de los entrevistados, "realmente nos hizo sentar cabeza y decir esto va enserio".

Así, cuando el país empezó a ser golpeado en el sector financiero, lo cual afectó el corazón económico de la sociedad, al no poderse hacer transacciones, hizo tomar conciencia y decir (al igual que el entrevistado) "hay que ponerse serio con esto". En este contexto es cuando el país comenzó a darse cuenta que tenía que acelerar todos los procesos y tomas de decisiones sobre el tema. En opinión de los entrevistados, venían haciéndose cosas, pero ahí tomó más fuerza el centro de respuestas a incidentes de seguridad informática que posee el país a través del Ministerio del Interior como un órgano coordinador de otros centros de respuestas de incidentes informáticos que se han ido conformando en los otros Ministerios; también se publican las políticas de ciberseguridad, ciberdefensa, se ratifica el convenio de Budapest, aparece un instructivo presidencial del año 2018 donde se comienza a exigir a las empresas que tengan oficiales de seguridad de la información, oficiales de protección de datos; también se empiezan a hacer actualización de leyes (aún no promulgadas pero ya se hallan en el Congreso): actualización para la Ley de Delitos Informáticos, actualización para la Ley de Protección de Datos, Ley de Ciberseguridad, Ley de inteligencia artificial, Legislación sobre los temas de teletrabajo y, la creación de una Dirección de Ciberseguridad a nivel país.

En el caso colombiano, se reconoce y valora la importancia del quinto dominio, al mismo tiempo que se considera un anhelo alcanzar la paz en el mismo, particularmente por la historia del país vinculada a su conflicto interno; sin embargo, el manejo de este conflicto interno les demanda un porcentaje importante del tiempo. Las fuentes entrevistadas

consideran que el país y sus actores son conscientes de los conflictos internos y externos generados en el quinto dominio, donde el ciberespacio se halla muy interrelacionado y conectado con su realidad, sin embargo, para ellos, es un área donde los conflictos no son tan visibles como en los otros dominios. Los especialistas consultados, consideran desde la óptica de este país, que en pocos años las guerras no serán ni en superficie, ni en mar, ni en aire, sino que tendrán como protagonista al quinto dominio y para ello el país utiliza una metodología, unas actividades antes de, para evitar tener un conflicto ciberespacial.

Respecto a la bibliografía, no reconocen haber leído artículos o libros que traten sobre la paz en el quinto dominio. Algunos de los entrevistados mencionan haber participado recientemente en cursos de la OTAN, de reentrenamientos con la Junta Interamericana de Estados Unidos, han participado en foros y centros de formación sobre ciberdefensa, ciberseguridad y les llama la atención no haber escuchado nunca sobre la paz en el quinto dominio (o cómo pensarla, gestionarla, etc.); sino que se tocan temas operacionales, de mantenimiento, temas tecnológicos, de capacitación de recursos humanos.

Pensar los Recursos Humanos para la ciberdefensa

En opinión de los especialistas consultados, no se conoce producción académica referida a los Recursos Humanos para la ciberdefensa en Brasil. En cuanto a la apreciación geopolítica del país sobre este eje, consideran que la Defensa Cibernética no existe sin recursos humanos capacitados, motivados y entrenados. La nación que sepa emplear de la mejor manera sus Recursos Humanos en esta área, tendrá mayor posibilidad de éxito en una eventual campaña militar cibernética, por ello la importancia que el país le da a la formación y obtención de este componente. En cuanto a la importancia estratégica de los Recursos Humanos para la ciberdefensa, la visión brasilera es que el tiempo necesario para calificar los Recursos Humanos y la relevancia del talento individual son esenciales para la creación de programas de entrenamiento y de valoración o estímulo a los profesionales que se desempeñan en la defensa cibernética. En Brasil los Recursos Humanos para la ciberdefensa son pensados y definidos, en el caso de la Defensa, por cada Fuerza Específica que es quien define sus propios recursos humanos. En el ámbito del Sistema Militar de Defensa

Cibernética (SMDC), el Comando de Defensa Cibernética (ComDCiber) actúa como órgano de asesoramiento a los respectivos Comandantes de Fuerzas en cuanto a la necesidad de Recursos Humanos para el sector.

Las fuentes chilenas que participaron de esta investigación, tienen la percepción de haberse dado cuenta, con el transcurrir de este último tiempo, que los Recursos Humanos en ciberseguridad, tiene una mayor demanda. En ese sentido, consideran que es un gran desafío, no solamente para Chile, retenerlos y cómo, particularmente son especialistas y escasos. En el sector público hay una fuga de estos talentos precisamente por la falta de incentivos y, no solamente monetarios, sino por capacitaciones, oportunidades de perfeccionamiento, oportunidades de intercambio. Entonces, en opinión de los entrevistados, es difícil competir cuando hay una demanda del sector privado donde los incentivos son muchos mayores. Por ello, hoy día hay todo un análisis de cómo va ser la estrategia para retener al talento ciber en el sector público de Chile. Por otra parte, lo que se está tratando de configurar es que exista una suerte de servicio militar, **pero un servicio militar orientado al ciber, mirando el modelo que tiene Israel, el cual fue también seguido por los alemanes.** Pero un servicio militar en esta área tiene otras aristas desde el punto de vista ético, del punto de vista de dónde operarían estas personas, entonces también es un tema que está pendiente –en opinión de los entrevistados- desde la perspectiva política para ver cómo se podría llevar adelante las propuestas, modificaciones y/o adecuaciones necesarias.

En resumen, respecto al asunto de los Recursos Humanos, para el caso chileno, actualmente existe una alta demanda, porque dieron cuenta que no había tanto personal para ciber, para cubrir toda esta demanda, sobre todo con la aceleración del tema con la pandemia. No obstante, existió un fenómeno regional, una fuerte llegada de migrantes, que han cubierto las áreas de tecnología por la escasez de profesionales chilenos. Surge así un desafío, una deuda política, académica, institucional, de cómo generar incentivos sobre todo en el sector público para retener a las personas, no sólo con un incentivo salarial sino también intangible.

En el caso del Ejército Colombiano, hace ocho años tuvieron una alianza con una multinacional de Estados Unidos mediante la cual empezaron a realizar los perfiles tanto académicos como operacionales de las personas que deberían trabajar en este ámbito. Hace 10 años en Colombia se empezó con la creación de lo que es la Ciberdefensa, que antes se llamaba seguridad de la información; según los entrevistados, aquella sección estaba integrada por ingenieros de sistemas rasos con algunas pocas especializaciones. Con la nueva exigencia y demanda de lo que hoy es la ciberdefensa, se dieron cuenta que no contaban con gente preparada según los requerimientos específicos que el nuevo ámbito de la defensa demandaba, entonces se reunieron con la Universidad de los Andes. De este modo, el Decano y el Jefe Militar de esta área, comenzaron a interactuar para poder contar con el personal adecuado. Los decisores políticos y académicos se reunieron con el presidente de la multinacional mencionada y al ver que no existía un perfil, empezaron a crear un grupo que se llamó GTDE (Grupo de Transformadores Digitales del Ejército). "Quisimos compararlos con un grupo especial pero que fueran de transformadores, de diseñadores, de programadores, de perfiles definidos en ciber, pero que trabajaran en el quinto dominio" dice uno de los especialistas entrevistados. Respecto a su diagnóstico inicial, cuando empezaron a trabajar en la definición y formación de los Recursos Humanos para la Ciberdefensa, contaban sólo con 4 personas que tenían maestrías, de los cuales dos habían hecho maestría en la Universidad de Talín (en el Centro Especializado en Ciberdefensa). Al respecto uno de los especialistas narra: "para poder tomar una decisión, como no sabía del tema, pues me tocaba decirle ¿usted qué opina?, hágame el diseño de…, tráigame una propuesta de línea de madurez… y dije ¡No!". Frente a esta realidad y con la alianza que hicieron con la mencionada empresa, consiguieron becas y presupuesto para 20 personas. "Imagínate, de un Ejército de 320 mil personas en ese entonces, escoger 20 personas talentosas para poder trabajar en esa parte ciber, todo un desafío. Entonces empezamos estudios socioeconómicos, psicológicos, de competencias y saberes, etc., y escogimos 20 personas entre oficiales, suboficiales, civiles, los agrupamos y los llevamos fuera, a capacitarse durante un año en la Universidad de los Andes".

Para la experiencia colombiana, al pensar el personal para la ciberdefensa, es muy importante la capacitación permanente, pero aún más importante mirar la actitud y aptitud del personal, porque –según dice el especialista- para hacer un desarrollo de software hay que sentarse a trabajar sabiendo que no se obtendrá un producto en tres horas "como es costumbre demandar algo en el ámbito militar" (sic). El desarrollador puede dedicarle un año de ardua tarea y tenerlo incompleto o no tenerlo aún, o bien luego de un año se da cuenta que lo que está haciendo no es estrictamente la intención que tiene el jefe y debe reformular su trabajo. Por otra parte, para la concepción estratégica de Colombia, el desarrollo del software es la base fundamental de la ciberdefensa, porque normalmente los países latinoamericanos, se puede decir que más de un 85% todo lo adquiere –dice el entrevistado-. En el desarrollo de la ciberdefensa es necesario ver los fracasos operacionales, las lecciones aprendidas y por aprender, los aspectos negativos y positivos para las futuras operaciones y con todo eso desarrollar lo que se deba desarrollar. Después de este grupo de transformadores digitales que desarrollaron, ahora el Ejército forma en cuestiones ciber desde la Escuela Militar. Desde que entran a los 17 años, ya hay un área de ciberdefensa y hay un área tecnológica para empezar a escalar en la temática. Estos les permite cambiar el chip en el componente humano vinculado a esta temática y eso es un salto cualitativo en cuanto a Recursos Humanos.

Hace ocho años, Colombia mediante su Escuela Superior de Guerra (Tanque de Pensamiento Estratégico del gobierno –en opinión de los especialistas consultados-) empezó a crear la Maestría en Ciberseguridad y Ciberdefensa de la región, "ni siquiera Estados Unidos tenía una Maestría como esta" –dice el entrevistado- En este proceso, la Escuela se unió estratégicamente con el Ministerio de Comunicaciones, el de Educación, el responsable de su armado viajó varias veces a observar la infraestructura educativa de varias universidades en los Estados Unidos. Actualmente van en la décima cohorte en la cual participan personas que tienen perfiles de jefes tecnológicos en las principales industrias y empresas del software, empleados de alcaidías, fiscalías, de diferentes ministerios del gobierno nacional, todos tomadores de decisiones. Es gente con una formación muy amplia, diferente a la maestría, que vienen trabajando hace unos 10 años en todo lo que es TICs y

puestos representativos a nivel nacional –comenta la fuente consultada-. En 2019 la maestría realizó un seminario en el que participaron todos los países de la región, en el mismo se miró la sinergia de la ciberdefensa en pos de los agentes generadores, es decir la unión de todos. Porque, de acuerdo a la opinión de los entrevistados, "en ciberdefensa si usted trabaja atomizado y solo, está muerto".

Puestos por sector en ciberdefensa

Los especialistas brasileros consultados no conocen producción académica que aborde la temática de puestos por sector para la ciberdefensa en Brasil. Al mismo tiempo, consideran que la definición de los puestos debe considerar también los procesos imaginados para el sector y la estructura necesaria de acuerdo a las definiciones estratégicas y las políticas del sector, como también a las demandas de especificidades técnicas, tecnológicas, políticas y operacionales. De acuerdo a esto, sostienen que los puestos en defensa cibernética deben ser ocupados por profesionales, los más calificados, que posean conocimiento y experiencia en las áreas de actuación. Las Fuerzas Armadas, bajo asesoría del ComDCiber, establecen los puestos para la defensa cibernética en el ámbito del SMDC. En el caso de Colombia, dos publicaciones contribuyen a la discusión de puestos por sector en relación a la ciberdefensa, son dos manuales a nivel de país, uno se llama "la ciberdefensa dentro de la infraestructura crítica del país" y, el otro se denomina "la ciberdefensa dentro de la infraestructura crítica de la ciberdefensa". De este modo, Colombia concibe catorce puntos para los cuales define el concepto de puntos críticos: la parte de gobierno, defensa nacional, seguridad tecnológica, todo lo que es el factor energético, minería, agricultura; y dentro de cada uno de esos catorce puntos críticos del país está inmersa la ciberdefensa con sus puestos.

Chile cuando empieza a construir su modelo, mira a España fundamentalmente, pero también se nutre del modelo de Israel, en particular porque consideran que en esta temática "no hay una bala de plata que nos sirva para cubrir todo", de Israel reciben apoyo y orientaciones al igual que de Estados Unidos. Según los especialistas entrevistados, hay bastante literatura gris, no difundida, sobre el tema de puestos por sector que va de la mano

con el eje de los perfiles profesionales. Chile llevó adelante estudios a través de la Academia Nacional de Estudios Políticos y Estratégicos (ANEPE), sobre cómo podría abordarse, en las organizaciones, el tema ciber. La conclusión a la que arribaron fue que el tema ciber se tiene que enfrentar a través de lo que son las amenazas y estas amenazas deben tratarse por momentos, donde hay un antes, un durante y un después. Estos momentos son radicales a la hora de ver la especialización que se necesita que incorporar en el mundo ciber, porque para el modelo chileno, todo lo que se refiere al modelo del antes está relacionado con la ciberdefensa, y la ciberdefensa engloba todos los sistemas de protección llámese sistema criptográfico, sistema de comunicaciones, etc.; entonces la expertise de la persona es muy específica dentro del mundo ciber, por eso ocupará un determinado y muy puntual puesto, con escasa rotación. El tema ciber, para el modelo chileno y en opinión del entrevistado, se asemeja a la medicina, donde hay aspectos y profesionales generalistas, pero también otros altamente especializados en diferentes temas o ramas. Luego viene el durante, es cuando se está efectuando el ataque, por lo tanto, ahí tienen que estar todos los especialistas en medidas de contraataque, malware, temas de ofuscación para el tratamiento de malware, etc. Por lo tanto, todo el personal que está ahí en el momento y durante el ataque, que para el modelo chileno es concebido como ciberataque o defensa activa, tiene otra expertise y otra demanda diferente al momento anterior. Finalmente, todo lo que es el después, es el tema forense, es donde se hace reconstrucción de escena, recuperación de activo, pericias forenses y por ello mismo, tienen otra especialidad. De este modo, en el modelo chileno, el momento te da la expertise que debe tener la persona. Todo esto, para que funcione, debe estar soportado por lo que ellos llaman ciberingeniería; los ciberingenieros son los que están encargados por ejemplo de la administración de la base de datos, del soporte, de todos los tipos de planes como por ejemplo los de contingencia, los de recuperación de desastre, de continuidad de negocio, los proyectos de innovación, entre otros. Esto tiene una lógica dado que, el personal por ejemplo de ciberdefensa, no está preocupado del soporte; así entonces, los profesionales que trabajan en ciberingeniería son los que aseguran que funcionen las otras tres áreas o momentos: la ciberdefensa, el ciberataque y el trabajo forense. El modelo considera que en conjunto con ello debe haber otra área, que es la ciberinteligencia, ésta se va a alimentar de datos de distintas fuentes y se alimenta a su vez

de otros ámbitos como la ciberingeniería, la ciberdefensa, el ciberataque, la forencia porque la ciberinteligencia es la que recoge los datos para transformarlos en información.

De este modo, hay un nuevo grupo de especialistas que más que nada son científicos de datos, informáticos pero orientados al análisis de datos e información, que a su vez son los que van a alimentar otra área denominada ciberoperación. El personal de ciberoperaciones son los que en su conjunto van tomando las decisiones para mitigar por ejemplo todo lo que son los perfiles de amenazas y cómo hago frente a ese perfil de amenazas; se ocupan también de las maniobras disuasivas, etc. En tal sentido, los que trabajan en el ámbito de ciberoperaciones tienen una formación mucho más directiva que el resto. Todo este conjunto de momentos y áreas es lo que el modelo chileno llama ciberseguridad, donde para ellos la ciberseguridad es el todo, la unidad es la ciberseguridad mientras que la ciberdefensa es una parte, es lo que trabaja en el antes y la ciberseguridad es el concepto global.

Perfiles profesionales orientados a la ciberdefensa

Los especialistas brasileros consultados, concuerdan que no disponen de información acerca de producción académica sobre perfiles profesionales orientados a la ciberdefensa de Brasil. Por otra parte, mencionan que en este país los perfiles profesionales son establecidos en el ámbito del SMDC. Asimismo, se puede decir que, desde la postura geopolítica de Brasil, consideran que el país necesita definir los perfiles y asociarlos a la educación y al entrenamiento necesario para obtener Recursos Humanos que ocupen los puestos establecidos de acuerdo a las definiciones técnicas, operacionales, profesionales y políticas establecidas, esto es una prioridad estratégica. En este sentido, para Brasil, la definición de los perfiles para la defensa cibernética constituye un paso fundamental para el establecimiento de estructuras adecuadas para la defensa del país en el quinto dominio.

Chile por otra parte, como se comentó en el apartado anterior, llevó a cabo una intensa investigación académica para definir las estructuras y puestos necesarios en las áreas ciber de las organizaciones, a partir de los cuales surgen luego los perfiles profesionales requeridos. Los especialistas entrevistados concuerdan que en Chile el mercado de

formación, en cuanto a la oferta de carreras, certificaciones y capacitaciones, está cubierto. En temas de trabajo forense hay diplomados, certificaciones, maestrías; en el sector defensa también, cada fuerza armada tiene su academia donde está dictando cursos de seguridad específicos; también la ANEPE dicta cursos, diplomados, magíster etc., en distintas áreas vinculadas a estos temas. Las universidades también cuentan con ofertas de formación que cubren los perfiles requeridos por la cuestión ciber, definida en el país. Para los entrevistados, lo primero es, "cómo enfrento mi estructura organizacional en lo referido a este tema", al respecto el modelo chileno establece momentos como ya se mencionaron, un modelo que, en opinión de los entrevistados, puede llevarse tanto a niveles directivos como a niveles tácticos, en lo público y lo privado, "porque en definitiva es lo mismo que sufre una pyme o una gran empresa" en opinión de los profesionales consultados.

Para describir la visión colombiana respecto a los perfiles profesionales, reproduciré las voces de los entrevistados que a través de ejemplos didácticos hacen visible la forma colombiana de pensar el tema. "Si a esta altura del desarrollo del tema ciber, colocamos un teniente coronel, que puede ser una persona de 40 años, quien de pronto ha estado dentro del conflicto armado en la selva y, uno le entrega todo lo que es ciberdefensa, esta persona se va a enloquecer. O sea, ¿qué tiene que tener? Un perfil tecnológico, un perfil de analista, conocimientos de inteligencia, que es un C5, donde el último 5 es ciberdefensa pero incluye comando, control, comunicaciones, computación y encierra todo este conglomerado con la protección de datos. Si no sabe comunicaciones a los 40 años va a patinar, es difícil que empiece a aprender de cero a esa edad. Entonces decimos tiene que ser una persona muy técnica, muy estudiosa, una persona académica, inquieta y, lo que siempre se ha mirado es la misma actitud y la misma aptitud para desarrollar las tareas pertinentes que el puesto requiere. Hay gente sumamente preparada, con muchas capacidades, pero vienen y destruyen, no permiten que haya trabajo en equipo; entonces vemos la parte de la persona, su formación académica, su desarrollo en la carrera militar. Es una complementación de todo eso".

Capacitación de los Recursos Humanos para la ciberdefensa

En la concepción estratégica de Brasil sobre la formación o capacitación de los Recursos Humanos para la ciberdefensa, considera que los países deben poseer capacidad de capacitación del personal en protección cibernética, ya que es el área más completa y demanda atención inmediata. Las demás capacitaciones, en exploración y ataque requieren más tiempo y mayor pericia, que pueden ser adquiridos fuera del país y desarrolladas internamente con el paso del tiempo. Para el país, la capacitación de Recursos Humanos en ciberdefensa tiene importancia estratégica dado que consideran que los recursos humanos marcan la diferencia en el quinto dominio y, su nivel de formación establecerá el alcance y la eficacia de las acciones; por este motivo el Ejército Brasilero cuenta con centros de entrenamiento para capacitación de militares en todos los tipos de acciones cibernéticas.

En Chile la capacitación del personal en el área ciber, en el caso de las Fuerzas Armadas tiene unas líneas profesionales ya definidas. Los cadetes entran a las respectivas escuelas y toman una especialidad y, dentro de esas especialidades hoy día están tomando la línea de informática para después ir a las unidades específicas. También pueden entrar los oficiales a las academias, las cuales están dictando formación específica y aquellos pueden optar de igual modo por organismos como la ANEPE o las universidades, todo ello encuadrado con los convenios que hay entre universidades o instituciones formativas y las Fuerzas Armadas. Entonces estos oficiales se van a desempeñar en las áreas de ciberdefensa como peritos informáticos, van a estar trabajando en ciberinteligencia o en temas de ciber operaciones.

Así, cada persona va tomando su línea de carrera o desarrollo profesional, tanto en el ámbito militar como en el de las empresas. En tal sentido, los entrevistados y fundamentado en lo previamente explicitado, consideran que la capacitación de los recursos humanos en Chile es un tema que está resuelto, la demanda está cubierta y por el lado de las Fuerzas Armadas también hay ofertas con un amplio espectro de capacitaciones específicas. Los especialistas entrevistados coinciden en la siguiente afirmación “hay que dejar claro, que no hay un superhéroe capaz de cubrir todas las áreas en este tema. El tema tiene tanta

diversidad que en realidad uno tiene que tomar una especialización"; en tal sentido aclaran desde la experiencia que les da sus desempeños en el área "por la misma diversidad de especificidades alguien que se dedica a hacer trabajo forense es difícil que luego lo veas haciendo ciencia de datos, podría hacerlo, pero no va a ser experto ni en uno ni en lo otro, tendrá una concepción general pero no la expertise de dedicarse a una especialidad". Y detallan para que no queden dudas "la realidad en esta área es que el que se dedica a ciencia de datos, luego no va a estar configurando firewall". Las fuentes consultadas coinciden que en Chile se logró entender que hay un nivel de expertise tal que y, como se mencionó antes en el modelo planteado, Chile ha asimilado que la manera de abordaje tiene que ser específica y esta es la razón por la cual la demanda de profesionales en temas ciber ha aumentado, "porque ya no está este superhéroe que en el fondo hacia todo o sabía de todo". Cuando Chile se vio golpeado con una catarata de ciberataques, se dio cuenta que era un tema que lo iba a afectar, entonces también comprendió la necesidad de cubrir las diferentes áreas, donde ya no es válido el concepto de tener alguien que haga de todo o salte de un tema o lugar a otro, quien no entiende y define políticamente esto no tiene éxito en la defensa cibernética, comentan los entrevistados.

En Colombia en el ambiente ciber, le dan mucha importancia a la ciberinteligencia y por ello crearon la Maestría en Ciberinteligencia. Consideran que es una rama a nivel mundial donde se dan unas capacidades impresionantes de gente talentosa, donde hacen análisis de cuáles pueden ser los ataques que reciben y después de un ataque hacen un análisis de cómo pueden ser los posibles cursos de acción de defensa, además se estudia el proceso de toma de decisiones, del proceso de inteligencia, el proceso de ciberinteligencia. Con esto comenzaron a poder potenciar las capacidades atomizadas que tenían. Por otra parte, en la Escuela de Comunicaciones, cuentan con una especialización de ciberseguridad, es la parte táctica, donde se brindan las especializaciones a oficiales y suboficiales, personal al que le falta mucho techo para desarrollarse, pero al mismo tiempo para evitar que esa capacitación no se vaya a perder. En la experiencia colombiana un agente de ciber no se prepara en 5 años, se logra preparar en 10 años; por este motivo cuando el recurso humano de esta área le dice a sus jefes "me voy a retirar y todo el mudo –que no entiende del tema ni

tiene una visión estratégica y geopolítica- le dice pues retírese, el país está perdiendo unas fortalezas muy grandes" –en opinión de los especialistas consultados. En cuanto a capacitación, Colombia ya logró capacitar a más de 600 personas en el área. Hay gente que trabaja en la parte planeamiento, en la parte operacional, en educación, en lo técnico, en la parte estratégica o en la parte de análisis. "Creo que hemos crecido mucho, creo que es un ambiente que como en todo el mundo y en toda organización, si no llega a crecer, tiende a desaparecer" concluye el entrevistado.

Reclutamiento para la ciberdefensa

En la apreciación geopolítica sobre el reclutamiento de personal para la ciberdefensa, Brasil entiende que a través del mismo se pueden obtener talentos únicos para las acciones en el espacio que el país requiere; es por eso que todo el país debe poseer programas para la identificación y el reclutamiento de personal para actuar en la defensa cibernética. En cuanto a la importancia estratégica del reclutamiento consideran que teniendo en cuenta la rápida evolución del espacio cibernético y de las amenazas en este ambiente, uno de los grandes desafíos para los gobiernos ha sido la retención de talentos. En este contexto, el reclutamiento se revela como una herramienta eficaz para mitigar el riesgo del impacto de eventuales pérdidas de personal. Por esta razón el Ministerio de la Defensa y las Fuerzas Armadas tienen procesos de reclutamiento permanente de personal para diversas áreas de la defensa cibernética.

En opinión de las fuentes chilenas consultadas, el reclutamiento en el caso de las Fuerzas Armadas es mucho más fácil dado que disponen de estándares y en función de ellos van reestructurando sus plantas de personal año a año; además cuentan con la facilidad de mover a la gente. Sin embargo, la dificultad que tiene es que el personal del que disponen es casi exclusivamente uniformado, si bien puede haber una cuota civil, pero es muy acotada. En el caso del ámbito estatal civil, si bien se tiene conciencia del tema ciber y, se han abierto más plazas, el proceso ha sido más lento porque ha implicado aumentar las plantas administrativas y esto depende del Congreso que autorice y sancione estos cambios, de negociaciones políticas, hay temas de remuneraciones, hay zonas grises, etc., por esto

mismo se ha ido haciendo, pero de forma más lenta. Luego, en el sector privado es distinto, es un sector más dinámico y se ha ido estructurando acorde a las necesidades, se puede decir que hay mucha conciencia y facilidad de decisión en este último sector.

"Dentro de las Fuerzas Militares, después de haber tenido ese gran éxito del grupo de transformadores digitales, hay dos fases más de transformadores digitales" comenta la fuente colombiana. El reclutamiento en el caso colombiano, es un proceso donde se estudia a los posibles candidatos desde antes, observan su perfil y cuando tienen definido al candidato se le dice "usted es talentoso en esta parte, ¿quiere…?" En el proceso de reclutamiento colombiano, desde la perspectiva del entrevistado lo más importante es que el personal demuestre la misma aptitud y la misma actitud siempre, ya que, un profesional puede ser muy talentoso, pero demuestra ser una piedra en el camino, no lo llevarán a trabajar a un área donde lo primero que se necesita es el trabajo en equipo, cero envidias, que sea cohesionado, "porque más bien nos va a provocar una desunión y eso nos ha pasado" expresa el especialista consultado. Y esto lo aprendieron de la NASA, según relata la fuente, hace unos 20 años vino la NASA y se llevó gente talentosa, entonces las autoridades lo primero que preguntaron fue "¿ustedes que le miran?, ¿cómo definen a quién seleccionar?" y la respuesta fue que miran el ser. Si miran y tienen en cuenta la parte de formación-capacitación que es sumamente importante en esta actividad, "es un ingrediente fundamental, pero el ser es preferible al saber, a veces", concluye el entrevistado.

En Colombia normalmente se trabaja con porcentajes de incorporación, así en el área ciber hace 5 años el porcentaje de incorporación era del 2 % y fue elevado al 6% semestral, la incorporación de tecnólogos en el área de informática. En la escuela militar de cadetes se incorporan profesionales dentro de una rama, donde por la propia realidad del país, las ramas de especialidad van cambiando; entonces si tienen necesidad en la parte jurídica ese año se incorporan profesionales solamente jurídicos o médicos, etc. Este año el porcentaje de incorporación es del 3% para C5, es personal femenino, con formación en ingeniería en sistemas. Inteligencia del Ejército ha trabajado también esta parte creando una maestría que fortalece las capacidades de ciberinteligencia. Porque para el país son tres

capas que están dentro del concepto operacional a nivel doctrinario: ciberseguridad, ciberdefensa y ciberinteligencia.

El problema de fuga de personal al sector privado en el caso colombiano, tiene una primera observación de los especialistas entrevistados, el profesional del área ciber es muy buscado por las empresas porque es la forma como ellos pueden fortaleces sus procesos y esto sucede en todas las áreas. Al respecto y sobre la problemática tanto del reclutamiento como de la retención del personal lo ponen en palabras con el siguiente ejemplo "Cuando te retiras si hay una empresa esperándote y te ofrece 15 mil dólares para trabajar ¿te negarías? Pues esto pasa en esta área y otras como por ejemplo los pilotos; formar un piloto lleva 10 años y si el tipo se formó y luego no lo llaman, no le dan espacio, no le dan oportunidades y, de pronto lo llaman para trabajar en otro país o en una empresa privada, pues se va". Por esta razón es muy importante y estratégico contar con planes de desarrollo profesional, de incentivos y de fidelización del personal en esta área. Por esta razón en Colombia, en la parte ciber, el personal se queda, en general, porque tiene un espectro muy grande de capacitación, es un área donde la gente tiene muy buenos beneficios personales, tiene muy buenos jefes, el Ejército permite que estos profesionales se capaciten, les brinda becas, les otorga permisos, cuentan con ciertas libertades en sus tiempos. "Eso no lo va a encontrar en ningún lado, entonces yo creo que la gente lo piensa mucho antes de irse", comenta la fuente. El 90% de las personas que trabajan en el área ciber tienen permiso para ir a estudiar.

Los visitantes ven la exposición de ciberseguridad de la Semana de la Ciberseguridad de China 2021 en Xi'an (2022)

Conclusiones

De acuerdo a lo investigado, respecto a pensar la paz en el quinto dominio, desde la perspectiva geopolítica y estratégica de Brasil, sólo se puede lograr aquello a partir de acciones transparentes y basadas en la confianza mutua, sin embargo, éstas son acciones que no se dan espontáneamente, sino que tardan en construirse tanto en los ámbitos bilaterales como multilaterales. Para la visión chilena, esta paz está asociada a múltiples factores, donde la disuasión es el componente fundamental y para ello, entre otras acciones se debe mostrar lo que se tiene y con qué cooperación internacional se cuenta en el tema. En el caso colombiano pensar la paz en el quinto dominio es un anhelo que se reconoce y valora para el cual hay que trabajar previamente.

En cuanto a pensar los recursos humanos del área, Brasil considera que la defensa cibernética no existe sin recursos humanos capacitados, motivados y entrenados; por eso afirman que la nación que sepa emplear de la mejor manera sus recursos humanos, se colocará a la vanguardia en el tema. Para ellos, el tiempo necesario para calificar dichos recursos y la relevancia del talento son esenciales en la creación de programas de

entrenamiento y estímulo profesional. Para Chile, es un desafío común encontrar modelos para tener el personal formado, particularmente porque es especializado, escaso y con pocos incentivos en el sector público para evitar la pérdida de talentos. En la experiencia colombiana es muy importante la capacitación permanente, ellos comenzaron hace 10 años generando alianza entre el sector público, el académico y una multinacional estadounidense a partir de lo cual crearon un grupo de Transformadores Digitales como punto de partida en este tema. Por otra parte, para la concepción estratégica de Colombia, el desarrollo del software es la base fundamental de la ciberdefensa, por ello piensan en sus recursos humanos desde que entran a los 17 años a las academias militares donde comienza la formación y la carrera en el área.

Cuando hablamos de puestos por sector de la ciberdefensa, Brasil considera que la definición de los mismos debe contemplar los procesos imaginados para el sector, la estructura necesaria acorde a las definiciones estratégicas y políticas, como también las demandas de especificaciones técnicas, tecnológicas, políticas y operacionales. Para Chile, los puestos en ciberdefensa pueden pensarse a partir de tres momentos: el antes referido a la ciberdefensa, que tiene que ver con la protección, la criptografía, las comunicaciones, entre otros, luego el durante, concebido como ciberataque o defensa activa y, el después vinculado al trabajo forense; a ellos se debe agregar tres áreas más: ciberingeniería, ciberinteligencia y ciberoperaciones.

Si nos referimos a la capacitación del personal, Brasil considera que los países deben poseer capacidad de formar al personal en protección cibernética, ya que es el área más completa y demanda atención inmediata. Para ellos, las demás capacitaciones, en exploración y ataque, requieren más tiempo y mayor pericia, que pueden ser adquiridos fuera del país y desarrolladas internamente con el paso del tiempo. En Brasil, la capacitación de Recursos Humanos en ciberdefensa tiene una importancia estratégica en el marco de una política que concibe que los recursos humanos marcan la diferencia en el quinto dominio. Para Chile, la capacitación del personal, también es central, dado que su modelo se fundamente en la expertise de puestos, saberes y prácticas, por ello definen que el abordaje tiene que ser específico donde ya no es válido el concepto de tener alguien que

haga de todo o salte de un tema o lugar a otro. Finalmente, para la experiencia colombiana, un agente ciber demanda una preparación de 10 años; por este motivo dejar ir al personal ya formado o no contar con planes para su permanencia implica una gran pérdida en las capacidades y fortalezas del país.

Por último, la investigación hace visible la necesidad de contar con un programa para la identificación y reclutamiento del personal ciber en sus diferentes roles, tareas y funciones. Dado que se presenta como una herramienta necesaria y eficaz para mitigar el impacto de la pérdida de talentos; en tal sentido también *se deben contar con planes y programas de contingencia donde lo fundamental debe estar puesto en los incentivos tangibles e intangibles que fidelicen a los recursos humanos del área.*

Bibliografía

ÁLVAREZ VALENZUELA, D. (2018). "Ciberseguridad en América Latina y ciberdefensa en Chile". Revista chilena de derecho y tecnología, vol.7, no.1, jun. 2018. Disponible en https://scielo.conicyt.cl/scielo.php?pid=S0719-25842018000100001&script=sci_arttext. Consulta: 11 de junio de 2021.

AMIGO TOSSI, A. (2019). "Consideraciones sobre la ciberamenaza a la seguridad nacional". Revista Estrategia, 6, 2019: págs. 69-79.

ARANDA MORA, O. (2018). "Ciberseguridad y ciberdefensa: prioridad nacional postergada". Revista de Marina. 135, 965, julio - agosto 2018: págs. 45-48.

ARIAS TORRES, N. A. y CELIS JUSTINICO, J. A. (2015). Modelo experimental de ciberseguridad y ciberdefensa para Colombia. Bogotá: Universidad Libre, Facultad de Ingeniería, Programa de Ingeniería en Sistemas. Disponible en https://repository.unilibre.edu.co/bitstream/handle/10901/10904/TRABAJO%20DE%20GRADO%28Nicolas%20Arias%20y%20Jorge%20%20%20Celis%29.pdf?sequence=1&isAllowed=y. Consulta: 14 de mayo de de 2021.

BALMACEDA HOYOS, G. (2011). "El delito de estafa informática en el derecho europeo continental". Revista de Derecho y Ciencias Penales, 17: págs. 111-149.

BARRIA HUIDOBRO, C. (2020). "Cibergeografía o el salto de lo terrenal a lo digital: las posibilidades y riesgos de un mundo red". Revista Política y Estrategia N°135. Disponible en https://www.politicayestrategia.cl/index.php/rpye/article/view/814/476%C3%A7. Consulta: 11 de junio de 2021.

BARRIA HUIDOBRO, C. (2019). "La dimensión del ciberespacio: una propuesta de ciberseguridad". Cuaderno de Trabajo N°1. Disponible en https://anepe.cl/wp-content/uploads/2020/10/Cuaderno-de-Trabajo-N%C2%B01-2019.pdf. Consulta: 11 de junio de 2021.

CÁCERES GARCÍA, J. A. (2017). "Colombia, estrategia nacional en ciberseguridad y ciberdefensa". Disponible en Air & Space Power, 29, 1, 1er trimestre 2017: págs. 85-89.

CORTES BORRERO, R. (2015). Estado actual de la política pública de Ciberseguridad y Ciberdefensa en Colombia. Villavicencio: Universidad Santo Tomás, Facultad de Derecho, Especialización en Derecho Administrativo. Disponible en https://repository.usta.edu.co/bitstream/handle/11634/14032/2015rodrigocortes.pdf?sequence=1&isAllowed=y. Consulta: 14 de mayo de 2021.

CUJABANTE VILLAMIL, X. A., et. al. (2020). "Ciberseguridad y ciberdefensa en Colombia: un posible modelo a seguir en las relaciones cívico-militares". Revista Científica General José María Córdova, 18, (30): págs. 357-377. Disponible en http://dx.doi.org/10.21830/19006586.588. Consulta: 14 de mayo de 2021.

DI BENEDITTO, M. E. (2017). "Defesa cibernetica - seguranca para os sistemas ciberfisicos dos meios operativos de superficie". Revista Maritima Brasileira, 137, 4/6, abril-junho 2017: págs. 67-87.

GOMEZ, J. A (2018). ¿De qué hablamos cuando hablamos de una defensa moderna? Santiago: Ministerio de Defensa Nacional.

GOMEZ URRUTIA, J. A. (2016). "La defensa nacional en Chile: una visión del Ministro de Defensa Nacional de Chile". Air & Space Power, 28, 2, 2do trimestre 2016: págs. 4-9.

LAVERDE CASTILLO, R. y HERNÁNDEZ BEJARANO, M. (2021). "Ciberseguridad y Ciberdefensa en Colombia". Revista Avenir, 4, (2): págs. 25-36. Disponible en https://fundacionavenir.net/revista/index.php/avenir/article/view/106. Consulta: 14 de mayo de 2021.

LEIVA, R. (2018). "Ciberdefensa, ¿hacia un nuevo eje estratégico?". Revista Ensayos Militares, 3, (1): págs. 77 - 92. Disponible en http://www.revistaensayosmilitares.cl/index.php/acague/article/view/4. Consulta: 11 de junio de 2021.

LOPES, G. (2014). "Análise Exploratoria da Securitisacao Militar do Ciberespaco nos EUA, Brasil e Canadá". Security and Defense Studies Review, vol. 15, págs. 116-138. Disponible en https://www.williamjperrycenter.org/sites/default/files/publication_associated_files/SDSR%20Vol15.pdf. Consulta: 11 de junio de 2021.

LOPES CARNEIRO, A. S. (2016). "A defesa cibernética como extensao do papel constitucional das forcas armadas na defesa nacional", en VARIOS AUTORES. Ciberdefesa e ciberseguranca: novas ameacas a seguranca nacional. Rio de Janeiro: Escuela Superior de Guerra.

MARIN, J., et. al. (2019). "Modelo Ontológico de los Ciberdelitos: Caso de estudio Colombia". RISTI, E17, enero 2019. Disponible en

https://www.proquest.com/openview/ef48269d2b309b4657581d7bc7b8172a/1?pq-origsite=gscholar&cbl=1006393. Consulta: 14 de mayo de 2021.

MARTABIT TELLECHEA, P. (2019a). "Atribuciones en el ciberespacio: piedra de tope en el Derecho Internacional". Cuaderno de Trabajo N°14. Disponible en

https://anepe.cl/wp-content/uploads/2020/10/Cuaderno-de-Trabajo-N%C2%B014-2019.pdf. Consulta: 11 de junio de 2021.

MARTABIT TELLECHEA, P. (2019b). "Infraestructura crítica, usuarios y contenido: ¿Qué se busca proteger en el ciberespacio?". Cuaderno de Trabajo N°9. Disponible en https://anepe.cl/wp-content/uploads/2020/10/Cuaderno-de-Trabajo-N%C2%B09-2019.pdf. Consulta: 11 de junio de 2021.

MARTABIT TELLECHEA, P. (2018a). "Ciberterrorismo ¿Realidad o mito?". Cuaderno de Trabajo N°5. Disponible en https://anepe.cl/wp-content/uploads/2020/11/Cuaderno-de-Trabajo-N%C2%B05-2018.pdf. Consulta: 11 de junio de 2021.

MARTABIT TELLECHEA, P. (2018b). "Seguridad versus libertad en el ciberespacio. Cuaderno de Trabajo N°9". Disponible en https://anepe.cl/wp-content/uploads/2020/11/Cuaderno-de-Trabajo-N%C2%B09-2018.pdf. Consulta: 11 de junio de 2021.

NIÑO WILCHES, A. F. (2014). "Ciberespacio: nueva fuente de amenazas contra la seguridad nacional". Revista de las Fuerzas Armadas, Vol. LXXXVII, 230, (julio 2014): págs. 45-54.

OSPINA, M., y SANABRIA, P. (2020). "Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia". Revista Criminalidad, vol. 62, 2, mayo-agosto 2020, págs. 199-217. Disponible en http://www.scielo.org.co/pdf/crim/v62n2/1794-3108-crim-62-02-199.pdf. Consulta: 14 de mayo de 2021.

PINEDO HERRERA, C. A. (2015). "Desarrollo de grupos nacionales de alerta, vigilancia y prevención frente a amenazas cibernéticas", en ALDA MEJÍAS y SOUSA FERREIRA. La multidimensionalidad de la seguridad nacional: retos y desafíos de la región para su implementación. Madrid: Instituto Universitario General Gutiérrez Mellado.

PINTO, R. A., et. al. (2018). "Inteligencia de fuentes abierta (OSINT) para operaciones de ciberseguridad. Aplicación de OSINT en un contexto colombiano y análisis de

sentimientos". Revista Vínculos: Ciencia, Tecnología y Sociedad, vol 15, 2, julio-diciembre 2018: págs. 195-214. Disponible en https://core.ac.uk/download/pdf/229162221.pdf. Consulta: 14 de mayo de 2021.

PINZÓN BUENO, J. C. (2020). "Reflexiones sobre la modernización y el futuro de las fuerzas armadas de Colombia: visión 2030", en GRIFFITHS SPIELMAN y TORO. Desafíos para la seguridad y la defensa en el continente americano 2020 – 2030. Santiago: Athena Lab.

POLLONI CONTARDO, A. (2015). "Ciberseguridad: ¿estamos preparados?". Escenarios Actuales, 1 (abril 2015): págs. 17-30.

REALPE, M. E. y CANO, J. (2020). "Amenazas Cibernéticas a la Seguridad y Defensa Nacional. Reflexiones y perspectivas en Colombia". Seguridad Informática. X Congreso Iberoamericano, CIBSI 2020. Disponible en https://editorial.urosario.edu.co/pub/media/hipertexto/rosario/anexos/proyecto-cibsi/10_S7_ok.pdf. Consulta: 14 de mayo de 2021.

ROGER, R. M (2015). "Manejo y gestión de la información de inteligencia para la seguridad multilateral del ciberespacio - enfoques de los Estados Unidos y Brasil". Gestión de inteligencia en las Américas. Washington: Universidad Nacional de Inteligencia.

SÁNCHEZ BUSTAMANTE, C. (2013). "Colombia asume el desafío cibernético". Diálogo, vol. 23, 2: págs. 66-69.

SÁNCHEZ LOZANO, M. L. (2016). "Lineamientos de política en ciberseguridad y ciberdefensa: logrando la seguridad y defensa de Colombia en un mundo digital". Ciberdefesa e ciberseguranca: novas ameacas a seguranca nacional. Rio de Janeiro: Escuela Superior de Guerra.

SANCHO HIRANE, C. (2018a). Ciberseguranca e políticas públicas: análise comparada dos casos chileno e portugués. Lisboa: Instituto da Defesa Nacional.

SANCHO HIRANE, C. (2018b). "Ciberinteligencia: contextualización, aproximación conceptual, características y desafíos". Cuaderno de Trabajo N°1. Disponible en https://anepe.cl/wp-content/uploads/2020/11/Cuaderno-de-Trabajo-N%C2%B01-2018.pdf. Consulta: 11 de junio de 2021.

SANCHO HIRANE, C. (2016). "Ciberespacio bien público mundial en tiempos de globalización: política pública de ciberseguridad una necesidad imperiosa y la ciberdefensa como desafíos del siglo XXI". Ciberdefesa e ciberseguranca: novas ameacas a seguranca nacional. Río de Janeiro: Escuela Superior de Guerra.

VALDIVIA CERDA, V. (2020). "Hipótesis de conflicto en el espacio ultraterrestre. De la metageopolítica a la inteligencia espacial". Cuaderno de Trabajo N°3. Disponible en https://anepe.cl/wp-content/uploads/2020/12/Cuaderno-de-Trabajo-N%C2%B03-2020.pdf. Consulta: 11 de junio de 2021.

WITKER BARRA, I. (2020). "Ciberespacio e inteligencia artificial. Nuevos actores y nuevos procesos en los conflictos internacionales datacéntricos. Una perspectiva desde Chile". Antecedentes para el debate acerca de una estrategia de seguridad nacional. Santiago: Academia Nacional de Estudios Políticos y Estratégicos 2019.