Formación militar en ciberdefensa: apreciaciones exploratorias desde las ciencias sociales sobre España, Francia e Israel

Por Guillermo Rutz*

Resumen: Este artículo brinda aspectos exploratorios para la discusión de la formación militar en ciberdefensa, desde la perspectiva de las ciencias sociales, a partir de fuentes académicas, militares y diplomáticas de España, Francia e Israel, entrevistadas durante el año 2021. Se enmarca en el contexto de investigación de la Facultad de la Defensa Nacional, bajo el Proyecto UNDEFI "Paz y guerra en el ciberespacio: formación militar en ciberdefensa". Para ello primero realiza un recorrido por los antecedentes de producción académica en el tema; luego aborda, desde la perspectiva de las fuentes entrevistadas en cuanto a experiencias nacionales, visión estratégica y visión geopolítica del país, seis ejes de análisis: paz en el quinto dominio, pensar los Recursos Humanos, puestos por sector, perfiles profesionales, capacitación del Recurso Humano y reclutamiento, todos para la ciberdefensa.

Palabras clave: ciberespacio – ciberdefensa – formación militar – estrategia y geopolítica.

* Disponible en: [https://independent.academia.edu/GuillermoRutz]

Introducción

No podemos ignorar, desconocer, menospreciar el tema; creer que otros tienen que solucionar los problemas, que no tenemos responsabilidades (aunque sean meramente intelectuales). Necesitamos salir del estado de apatía, abrir los ojos de la conciencia intelectual personal y colectiva, buscar y proporcionarnos información y herramientas que nos permitan comprender de dónde venimos, dónde estamos y visionar-proyectar el futuro hacia dónde queremos-debemos ir, animándonos a ser libres o comprendiendo qué nos lo impide serlo.

Maniobras de distracción, entretenimiento, desinformación, sobreinformación, manipulación, adoctrinamiento, entre muchas otras que se podrían mencionar, son métodos en vigencia y de uso real para producir impactos concretos, según intereses específicos, en nuestros pensamientos y sentimientos, logrando con ello condicionar el comportamiento individual y colectivo. Podemos agregar, a los elementos de análisis social, las técnicas y dispositivos de vigilancia, los datos personales masivos que brindamos ingenuamente mediante los celulares, las redes sociales, los entornos virtuales laborales, bancarios o en cada acto de consumo diario conectado a sistemas virtuales, almacenados y usados por gigantes transnacionales de la información, a lo que se suman las tecnologías de seguimiento, geolocalización. Todo esto es lo que no podemos ignorar, ni sacarnos el lazo de la responsabilidad. Sobre los tópicos mencionados en este párrafo, sólo como ejemplo y no de forma excluyente, es que debemos comprender en las dimensiones sociales, políticas, económicas, militares… desde una perspectiva soberana y nacional.

Sin embargo, para el tema de la ciberdefensa, que es la mirada de este artículo, es necesario incluir la dimensión geopolítica y estatal de estas cuestiones. La guerra híbrida –que para algunos no existe, no quieren mencionar o les provoca aversión- pero que existe, dando lugar a la lucha por el control de poblaciones propias y ajenas; las operaciones de influencias –guerra psicológica- con campañas de manipulación a gran escala; las más variadas tecnologías –conocidas y las que no conocemos–, que juegan en el tablero del dominio mental, social y militar; forman parte sobre lo que debemos informarnos y conocer, para comprender y decidir. Porque si no sabemos a qué nos enfrentamos y no buscamos generar capacidades para enfrentarlo, difícilmente podremos correrno del papel de espectador al de protagonista.

Los desafíos, amenazas y retos del mundo hiperconectado en el que vivimos, junto a los cambios sociológicos, tecnológicos y geopolíticos afectan nuestras sociedades. Frente a esto surgen nuevos debates, posicionamientos e intereses que hasta el presente no habían sido

observados, analizados, registrados, interpretados desde lo académico. Creer que no tenemos nada para mirar de experiencias ajenas, que lo que sucede en otras sociedades y Estados no nos sirve porque no es autóctono, que nosotros lo podemos-sabemos todo y debemos evitar contaminarnos con lo proveniente de potencias bélicas o con capacidades y vocación defensiva, negándonos a conocer los errores, aciertos y el camino recorrido por las experiencias de fronteras afuera, es contradictorio al proceso científico y como mínimo un error estratégico, por mucha capacidad intelectual y pensamiento nacionalista que tengamos. Es por este motivo que este artículo plantea los resultados de una investigación exploratoria, cualitativa, de análisis de fuentes primarias y secundarias, que deja puertas abiertas para continuar profundizando, conociendo y aportando a la discusión del tema; cuya primera parte se publicó como "Formación militar en ciberdefensa: apreciaciones exploratorias desde las ciencias sociales sobre Brasil, Chile y Colombia", (Rutz, 2022).

En tal sentido, 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 Recurso Humanos, puestos por sector, perfiles profesionales, capacitación de los recurso humano y reclutamiento. Se incluye además un estado del arte, no exhaustivo, sobre las temáticas de ciberdefensa, ciberespacio y ciberseguridad, relativo a los países involucrados en el presente trabajo.

Antecedentes en la producción académica

En este apartado haré mención, de manera no exhaustiva y sin un análisis de los textos, a un recorte de bibliografía referida a los ejes de la investigación las que, por otra parte, fueron mencionadas o sugeridas por las fuentes entrevistadas. De este modo, doy cuenta de la existencia de estas.

Desde la perspectiva de España, respecto al eje 1: la paz en el quinto dominio se puede mencionar a Baños (2020) con "el dominio mental. La geopolítica de la mente", al igual que Gómez de Agreda (2021) "Mundo Orwell. Manual de supervivencia para un mundo hiperconectado". En el mismo sentido, sobre el eje 2: pensar los recursos humanos, es válida la lectura del texto "necesidad de una conciencia nacional de ciberseguridad. La ciberdefensa: un reto prioritario" publicación de la Escuela de Altos Estudios para la Defensa. En lo que concierne al eje 3: puestos por sector en ciberdefensa, se pueden mencionar a Pou Rodríguez

en “demanda en ciberseguridad, sector de pleno empleo”, como también Pastor Acosta y otros “seguridad nacional y ciberdefensa”.

En el punto 5: Capacitación del Recurso Humano para la ciberdefensa, la bibliografía española hace referencia a Fajón Chamorro “formar ciberguerreros”; Morales y Velázquez (2013) “la responsabilidad del mando en la conducción de las operaciones durante la ciberguerra: la necesidad de un adiestramiento eficaz”; González Cussac (2010) “estrategias legales frente a las ciberamenazas”; Gómez de Agreda (2012) “el ciberespacio como escenario del conflicto. Identificación de las amenazas. El cibespacio nuevo escenario de confrontación”; Ministerio de Defensa (2011) “ciberseguridad, retos y amenazas a la seguridad nacional en el ciberespacio”; Ministerio de Defensa (2013) “necesidad de una conciencia nacional de ciberseguridad. La ciberdefensa: un reto prioritario”. En la bibliografía se mencionan, además, otros textos recomendados por las fuentes españolas.

En el caso de Francia se puede mencionar a Cobo “las claves para comprender la estrategia cibernética francesa y sus riesgos”; Nocetti (2018) “geopolítica de la ciberconflictividad”; Gautier (2018) “las claves de la defensa y la seguridad de los franceses”; Géry (2018) “el derecho internacional y la proliferación de las armas cibernéticas”; o “estrategias de seguridad cibernética de los Países Bajos, Francia y Alemania”.

Paz en el quinto dominio

Para España, según las fuentes entrevistadas, el quinto dominio no es un dominio en el que se pueda hablar de paz. Las nuevas tecnologías y el desarrollo de éstas han traído un nuevo campo de batalla donde la mayoría de los Estados se enfrentan actualmente (aunque no lo admitan o no se dé a conocer): el ciberespacio. El mismo carece de fronteras, fue creado por el hombre y supone nuevas amenazas para los Estados, las empresas y los ciudadanos. En tal sentido, al no existir fronteras, ni leyes que regulen el ciberespacio, la guerra cibernética no es una guerra convencional, nos aclara una de nuestras fuentes; así, para que España se declare en estado de guerra debe aprobarse por mayoría absoluta en

el Congreso de los Diputados, sin embargo, esto no pasa en la guerra que se libra en el ciberespacio.

En este contexto, el Centro de Excelencia para la Ciberdefensa Cooperativa de la OTAN, en 2013 dio a conocer de manera pública lo que se conoce como el Manual de Tallin, el cual está basado en opiniones y recomendaciones sobre el acercamiento de la ciberguerra al Derecho Internacional y las responsabilidades de los Estados en los conflictos cibernéticos, nos aclara el entrevistado y amplía citando a Chema Alonso (Jefe de Datos de Telefónica y Presidente de Eleven Paths) quien sostiene que desde hace años los países han cometido agresiones sistemáticamente unos contra otros donde generalmente estas agresiones han sido gestionadas sin que los medios de comunicación tuvieran noticias de ellas, por ello, nuestra fuente, siguiendo a Alonso sostiene que ahora las guerras se combaten aún sin estar declaradas, sin el conocimiento de los medios de comunicación, sin todos los parámetros y condiciones de las guerras tradicionales. Esto constituye un nuevo orden en el mundo de la guerra, un nuevo orden dado por la realidad cibernética.

El origen de un ciberataque es muy difícil de averiguar, por eso la ciberguerra es tan misteriosa, opina nuestra fuente. En tal sentido, sigue citando a Alonso, en cuanto a que luego de un ciber ataque siempre hay especulaciones de quien creó tal o cual ciber arma u originó el ataque o que la mayoría de los países con capacidades ciber fabrican ciber-armas. Al respecto, además de los casos conocidos, de la entrevista surge el caso del Malware Careto, descubierto en 2014 por Kaspersky Lab y que de acuerdo a las declaraciones del Jefe de la unidad de inteligencia de Eulen Seguridad (Carlos Torres Blanco) el equipo que lo desarrolló tenía como objetivo atacar países de interés para España. Sin embargo, España también sufrió esta ciber-arma sin que esto signifique que los afectados fuesen embajadas o destinos diplomáticos españoles y, si lo fueron, podrían tratarse de objetivos de interés para el gobierno español, se explica en la entrevista.

Por lo tanto y, en el marco de lo descripto, para España, pensar la paz no es más que una utopía, según las voces de los propios entrevistados. Así, desde su perspectiva estratégica, todos los países están enfrentados en el ciberespacio, tienen aliados al igual que en los otros ámbitos. Pero aun siendo aliados también se espían unos a otros y, al mismo tiempo, trabajan juntos para conseguir objetivos de importancia estratégicas entre aliados, nos refiere una de las fuentes consultadas. En este sentido, comenta que uno de los países más desarrollados en ciberdefensa es la República Popular de China, siendo el propio gobierno chino quien reconoció en 2011 que entre las filas de su ejército se encontraba una ciber unidad militar. Luego en 2015 admitió que tenía divisiones especializadas en ciberguerra. Al respecto, el

especialista consultado, citando a Alonso, comenta que Estados Unidos publicó en 2013 un informe donde se afirma que China había robado, al gobierno estadounidense, diseños militares de importancia estratégica; esto es un ejemplo más de guerra cibernética. Argumentando la perspectiva estratégica mencionada y, apoyándose en Torres Blanco, menciona que Corea del Norte juega un rol importante en el ciberespacio, ya que en 2014 era considerada la tercera unidad de ciberguerra más grande del mundo, con dos grupos identificados: la oficina 91, la unidad 121, y seis mil efectivos activos. A su vez, Estonia cuenta con mucho tiempo de desarrollo e implementación de las TIC lo cual la convierte en un activo estratégico para el desarrollo de la ciberseguridad de la OTAN, por ello en 2008 se creó en Tallin un Centro de Coordinación de Defensa Cibernética.

Si bien para España los Estados han encontrado en el ciberespacio un tablero en el que enfrentarse sin declarar la guerra, también considera que sólo entre el 15 y el 20 por ciento de los ciberataques son dirigidos por Estados. Los lobos solitarios o las guerras asimétricas no se encuentran sólo en el mundo físico, dice nuestra fuente. Tanto los robos masivos de información en temas de Defensa Nacional, datos personales, investigación científica, financieros, económicos, en el ámbito público o el sector privado; como el ataque directo a objetivos estratégicos de un país hacen que el ciberespacio sea de gran importancia para diferentes actores tanto para atacar como para defender. Por esta razón, es considerado el quinto dominio de la guerra, junto a la tierra, el mar, el aire y el espacio, en opinión de nuestras fuentes españolas.

Francia desde su perspectiva geopolítica, piensa la defensa de manera global. El jefe de las Fuerzas Armadas es el Presidente de la República, a su vez el Primer Ministro es el encargado de la Defensa Nacional y cada Ministerio tiene un papel importante en relación a este tema; en tal sentido, para ellos, el quinto dominio puede tomar un objetivo en cualquier lado o ámbito: defensa, finanzas, interior, economía, o cualquier otro objetivo de la sociedad francesa como empresas, personas, infraestructuras y, puede alterar, atacar, espiar y por eso lo consideran un tema global no solo de la Defensa Nacional. Por tal motivo, cuentan con una política y una estrategia de ciberdefensa para el Ministerio de Defensa, pero también para el Ministerio del Interior a quien le compete el territorio interior de Francia. Así, cada ministro en Francia tiene un General, que es su vínculo con las Fuerzas Armadas, y es quien aconseja en estos temas. La Ciberdefensa para Francia es un tema global y de prioridad estratégica nacional.

En cuanto a la importancia estratégica de pensar acciones para la paz en el quinto dominio, Francia si bien no se considera a sí mismo un país expedicionario, sus Fuerzas

Armadas son desplegadas fuera de su territorio en función de acuerdos de defensa con otros países. Al mismo tiempo junto a Europa de donde forma parte, reciben amenazas permanentes, donde en palabras del Jefe de Estado Mayor Conjunto (citado por el entrevistado) "el mundo cada vez se vuelve más salvaje, confirmado por los teatros de operaciones recientes: Afganistán, Irán, Malí…). Sobre el particular, y de acuerdo a nuestra fuente, para Francia la guerra es cada día más compleja, global, híbrida, donde los demás países también utilizan todo el entorno ciber para atacar, por lo cual la ciberdefensa es de importancia estratégica para el país. Si bien Francia no usa lo ciber para atacar –aclara el entrevistado- sí lo usa para defenderse, con la certeza que otros países tienen doctrinas de uso de lo ciber para el ataque y cuentan con mucho personal, con fuerzas muy grandes dedicadas exclusivamente a lo ciber y por ello es una necesidad y una realidad tener que prepararse en el tema. Al momento de la entrevista, la fuente consultada afirma que la decisión de Francia es prepararse sola, en confidencialidad, por lo cual no tiene acuerdos de cooperación en formación o entrenamiento ciber con otros países.

En relación con esta última idea del párrafo precedente, se pueden mencionar como ejemplo algunas de las diferencias entre Francia y la OTAN en el marco del Manual de Tallin. 1- la teoría de los expertos que escribieron ese manual consideran, respecto al Estado cuyo territorio es utilizado para hacer un ciberataque, si ese Estado no quiere o no puede tomar medidas contra los que son responsables de esa agresión, el Estado que es víctima puede actuar contra el Estado que no hace nada, esta es la visión de Tallin. Sin embargo, para Francia "…el Estado víctima puede activar mecanismos a nivel sólo político y diplomático y por ejemplo hablar con el Consejo de Seguridad de las Naciones Unidas, pero la legítima defensa no podrá ser invocada por el Estado víctima". 2-Otro ejemplo es la diferencia en la definición de un ciberataque en conflicto armado. Para Tallin el ciberataque es una ciberoperación ofensiva o defensiva que razonablemente puede causar heridas corporales o la muerte, daños materiales o destrucción a infraestructuras. Para Francia, un ciberataque en conflicto armado constituye un ataque a partir del momento en que los equipamientos y los sistemas que son afectados pueden no servir (o ser inutilizados) para aquello en lo que debían servir, de manera permanente o temporal y cuyos efectos no se pueden revertir. En el caso de efectos temporarios o reversibles el ataque es caracterizado donde la intervención del adversario es necesario para herir la infraestructura y/o el sistema. 3-También tienen diferencia en la distinción de conflictos armados y la calificación de datos civiles en conflictos armados. Para Francia, su estrategia de Ciberdefensa es clasificada, sin embargo, hay una política ministerial de lucha informática llamada "Política Ministerial de Lucha Informática Defensiva" del Ministerio de Defensa, que es pública.

Para Israel, en cuanto a trabajar en aspectos geopolíticos que contribuyan a la paz en el quinto dominio, consideran que siempre hay riesgos. Sostienen que Irán, China, Rusia usan lo ciber en ámbitos como seguridad, negocios y otras maneras; sin embargo, para nuestra fuente Israel tiene una buena fuerza en temas de defensa y ataques ciber. El punto de vista del entrevistado no concuerda con la tendencia actual de considerar que en cada cosa del mundo o de la vida cotidiana esta lo ciber, sino más bien hay que conocer, focalizar y hablar de tres temas centrales en el ámbito ciber: la ciberdefensa, el ciberataque y la ciberinteligencia. Ciberdefensa, es decir, cómo se hace seguridad para los intereses nacionales y todos los modos estratégicos del ámbito ciber; entender lo que pasa en otro lado, que pasa con tus potenciales enemigos y hacer lo que se necesita hacer para defender tus entornos estratégicos. Lo segundo es conocer todo lo relativo al ciberataque para reconocer debilidades, pensar estrategias y desarrollar capacidades. Y lo otro es la ciberinteligencia, la cual sirve para todo y todos los ámbitos de interés nacional (económico, social, militar, estratégico…) el país tiene (o debe tener) la inteligencia, en este caso la ciberinteligencia, para entender los riesgos, las oportunidades, entender lo que necesitas conocer de vos y del afuera, entender cómo y cuándo necesita atacar y si lo puede hacer. De los tres aspectos a conocer y manejar en el ámbito ciber, el más básico y el más importante es la ciberinteligencia, desde el punto de vista de Israel. Entonces, nos dice nuestra fuente, "también en temas de unidades hay unidades de defensa, hay unidades que hacen ciberinteligencia y hay unidades que hacen entienden en lo relativo al ataque. Pero en la misma oficina de la inteligencia, todos saben todo lo que pasa y cada uno tiene su responsabilidad".

Pensar los Recursos Humanos para la ciberdefensa

Francia afirma que se halla pensando en todas las cuestiones que hacen al tema de los recursos humanos para la ciberdefensa, donde por ser un comando joven, entre otros aspectos hay que encontrar los cuadros y los mandos que puedan crear una estructura idónea y de acuerdo con las necesidades y políticas del país. Nuestra fuente, nos explica que luego de contar con la estructura, cuadros y mandos surge la tarea de reclutar, ¿de dónde? de aquellos ámbitos donde se forman los informáticos, buscan aquellos profesionales que acrediten los más altos niveles posibles de conocimiento y experiencia en las cuestiones que el perfil requiera. A continuación, se trabaja sobre operaciones, innovaciones y recursos en cada polo de competencias de ese agrupamiento, lo cual comprende entrenar, desarrollar, conocer sobre estrategia, innovación, recursos, operaciones, entre otras cuestiones.

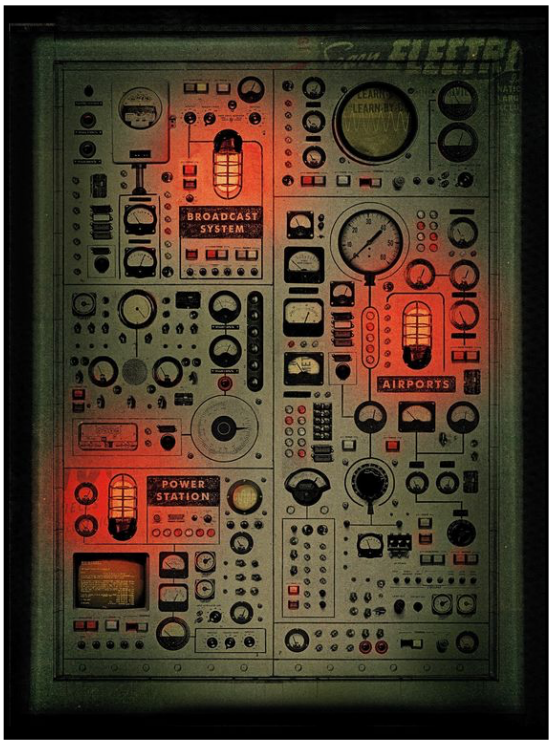
Para Francia, pensar los recursos humanos para la ciberdefensa tiene una importancia estratégica real y actual, dado que éstos van a ser muy importantes debido a que es un

agrupamiento muy técnico y se los necesita con el más alto nivel de formación, entrenamiento, capacidades, mucho más que otro tipo de unidad. "Se necesitan técnicos altamente capacitados –nos dice el entrevistado- por eso imagino que dentro de los tres mil quinientos cibercombatientes (número actual con que cuenta Francia) son todos de un nivel de conocimiento y formación muy alto, no soldados sino oficiales y suboficiales". Si bien el número actual de cibercombatientes con que cuenta Francia es de 3.500, su objetivo es aumentar sustancialmente esta cifra debido a que la ciberdefensa y el COMCIBER es una de las grandes prioridades de la Ley de Programación Militar 2019-2025 de Francia. El país tiene desde hace 7 años un Comando Ciber (COMCIBER) y desde hace aproximadamente 2 años cuentan con un agrupamiento que depende del COMCIBER. En este contexto y en relación a los recursos humanos, se puede decir que este Comando cuenta con su propio Estado Mayor y un agrupamiento con 4 centros técnicos: el centro de análisis y lucha defensiva informática, el centro de control de la seguridad de los sistemas de información, el centro conjunto de homologación principal y el centro de preparación operacional de ciberdefensa.

En el caso de Israel, ellos entienden que el tema ciber es uno de los más importantes hoy en día. En palabras de nuestra fuente "puedes decir tengo muchos soldados, pero al final lo que gana la guerra es el componente ciber"; entonces en este contexto y desde esta perspectiva es muy importante como se piensa, se define y se implementa todo lo relativo a los recursos humanos. Israel piensa, además, esta importancia, desde el punto de vista de la inteligencia porque para ellos, sin inteligencia no puedes defender, no puedes atacar, no puedes pensar el futuro, no puedes hacer nada. Por ello, nos dice el entrevistado junto a otras aclaraciones, que el tema de ciber inteligencia es el más importante, también en cuanto a los recursos humanos. Por otro lado, en el caso de Israel, cuando alguien conoce del tema, termina yendo a la mejor empresa ciber del mundo. Así luego sale con todo el conocimiento y la mejor experiencia; experiencia que no tienen en otros países porque Israel está en un conflicto permanente, con enemigos activos en tiempo real, con fronteras activas y calientes; por todo esto la experiencia que adquieren en este país es muy importante y de alta calidad (de acuerdo a la fuente consultada).

El tema del personal es el más importante para Israel en lo relativo a lo ciber, es por esto que empiezan a prestarle atención y ocuparse desde el colegio secundario a partir de los 15 o 16 años, donde comienzan a estudiar algunos temas. En tal sentido, cuentan con unidades ciber que apoyan los planes de estudios en estos niveles, para que al final los que terminan el secundario salgan con el conocimiento básico en el tema. También se hacen exámenes de temas ciber al finalizar los estudios secundarios donde las unidades ciber del

gobierno son expertas en cómo hacer los exámenes y cómo atraer a los mejores estudiantes. Por otra parte, nos ilustra el entrevistado, que cuando ingresan al ejército, tienen un conocimiento muy básico y para llegar a un conocimiento más profesional hay cursos que realizan en la misma unidad que entran.



Puestos por sector en ciberdefensa

Para España, cubrir puestos en el área de ciberseguridad y ciberdefensa, es clave. En tal sentido, tanto la administración pública como los directivos de las empresas son cada vez más conscientes de la importancia de la seguridad informática. Los medios de comunicación especializados como SFGATE[1], en su artículo "Demand to fill cybersecurity Jobs booming" señala que en los próximos 10 años el número de puestos relacionados con la seguridad de la información se multiplicará por 10. España entiende que los profesionales de este ámbito son necesarios en empresas de diferentes sectores, como el financiero, el comercial, la educación, los ámbitos del gobierno y todos aquellos donde la información y la tecnología informática estén presentes; por ello se espera también que el incremento en las contrataciones haga subir de igual manera los salarios. Lo que preocupa actualmente es que no haya suficientes personas preparadas para cubrir la demanda y es aquí donde adquieren relevancia como actores las universidades y las políticas de Estado. Ambos deben ser capaces de fomentar nuevos talentos y de mantener los estudios en seguridad TIC actualizados y a la vanguardia.

Ante la pregunta ¿Cómo describiría la importancia estratégica de pensar los puestos por sector en ciberdefensa?, la fuente consultada nos comenta que la importancia de cubrir estos puestos es crítica para el Estado, las empresas, el sector público y privado. De acuerdo a estadísticas del Ministerio de Trabajo español, el número de desempleados ha aumentado en 2021 hasta 3.964.353, cifra que supone un incremento interanual de más del 21%. Sin

[1] https://www.sfgate.com/

embargo, 8 de cada 10 directores de recursos humanos del país reconocen tener problemas para reclutar talento y los consultores de Adecco[2] han empezado a detectar que en promedio, un 9% de las vacantes disponibles quedan sin cubrir, porcentaje que en perfiles muy específicos y determinadas zonas geográficas, llega al 60%.

En este contexto, Adecco, compañía de gestión de recursos humanos realizó estudios de perfiles deficitarios en el mercado laboral de España y las razones de la escasez de talento en el país. De acuerdo con el mismo, si bien cada región tiene sus peculiaridades, hay perfiles que se ven más afectados por la escasez a nivel general, es el caso de los profesionales del ámbito IT (que llevan años siendo los puestos más difíciles de cubrir). Existen varias razones que explican la situación y tienen diferente origen y ámbito de actuación. Así, la escasez de perfiles altamente calificados y bien formados, los turnos cambiantes para determinados puestos, el dominio de idiomas donde cada vez más se solicita el manejo de una segunda y hasta tercera lengua, los salarios poco competitivos para posiciones concretas y en determinados ámbitos y/o regiones, búsqueda de candidatos muy especializados o perfiles muy técnicamente cerrados. La fuente consultada, cita a Rubén Castro, director de Adecco Staffing quien expresa que tenemos la generación mejor preparada de la historia, pero hay una parte de la población que se ha quedado colgada de ese nivel y puede reenfocar su carrera hacia estos perfiles y sectores. Ahora más que nunca el talento debe apostar por el reskilling[3] y el upsikilling[4] como vía para una mayor empleabilidad, concluye el entrevistado.

> Entre 75 y 375 millones de trabajadores (del 3% al 14% de la fuerza laboral mundial) deberán cambiar de categoría ocupacional para 2030 debido a la automatización, la inteligencia artificial y la digitalización, según el estudio 'Jobs lost, jobs gained: workforce transitions in a time o automation' elaborado por McKinsey Global Institute. De ahí que cobren especial importancia conceptos como 'reskilling' y 'upskilling', que siempre han existido en la empresa. "Son lo que se denominaba reciclaje o promoción continua", recuerda Elisabet Bierge, socia y directora de negocios de AdQualis Executive Search.[5]

[2] The Adecco Group es una compañía de recursos humanos con base en Zúrich, Suiza. El Grupo Adecco da trabajo a aproximadamente 700.000 trabajadores con contratos temporales y cuenta con más de 34.000 empleados propios y 5.200 oficinas en más de 60 países y territorios alrededor del mundo. https://www.adecco.es/

[3] El reskilling, también conocido como reciclaje profesional, busca formar a un empleado para adaptarlo a un nuevo puesto en la empresa.

[4] El upskilling busca enseñar a un trabajador nuevas competencias para optimizar su desempeño.

[5] https://www.bbva.com/es/reskilling-y-upskilling-renovarse-en-tiempos-de-incertidumbre/

Respecto a la definición de puestos para la ciberdefensa en España, el Mando Conjunto del Ciberespacio, encargado de la ciberdefensa de las redes de comunicaciones militares, propone los puestos de trabajo y son aprobados por el Estado Mayor Conjunto. El Mando Conjunto del Ciberespacio está encabezado por un General de División, tiene un segundo comandante, de nivel General de Brigada y, seis Jefaturas al mando de Coroneles entre las que cabe mencionar la Fuerza de Operaciones en el Ciberespacio, cuya misión fundamental es realizar acciones de defensa, inteligencia y respuesta en el cibespacio, siendo también la responsable del equipo de respuesta a incidentes del Ministerio de Defensa (ESP-DEF-CERT). En el resto de los ámbitos estatales los CERT de referencia son el del Centro Nacional de Inteligencia (CNI CERT) y el del Instituto Nacional de Ciberseguridad (INCIBE CERT).

En el ámbito civil de la ciberseguridad, el gran número de amenazas cibernéticas, "la escasez de profesionales con habilidades suficientes"[6], como también los salarios competitivos y las descripciones de trabajo interesantes a los que se enfrentan, son algunas de las razones para elegir una carrera en el campo de la ciberseguridad, afirma el entrevistado. Sin embargo, decidir qué camino seguir puede resultar abrumador, sobre todo porque hay muchos perfiles en los que es posible desarrollarse, cada uno con sus requisitos y habilidades específicas; también es importante tener en cuenta que para ocupar esos roles "no siempre es necesario contar con un título universitario"[7], concluye nuestra fuente. A continuación, se mencionarán algunos de estos puestos por sector de la ciberdefensa que son considerados desde la perspectiva de nuestro entrevistado.

Administrador de Sistemas. El administrador de sistemas es en realidad una de las profesiones más importantes en el camino hacia la carrera de ciberseguridad. Cyberseek[8], un sitio que proporciona una variedad de información acerca de la planificación de carrera en ciberseguridad ubica el rol del SISADMIN en el área de profesionales que se dedican a las redes informáticas y como una posición que funciona como la puerta de entrada para ocupar posiciones más específicas en el campo de la seguridad. Esto significa que los administradores de sistemas no se describen estrictamente como profesionales de la ciberseguridad, sin embargo, necesitan tener importantes conocimientos en seguridad para realizar su trabajo, tal

[6] https://www.welivesecurity.com/la-es/2020/11/03/falta-profesionales-ciberseguridad-brecha-que-crece/

[7] https://www.welivesecurity.com/la-es/2019/11/11/profesionales-en-seguridad-informatica-entre-la-formacion-academica-y-la-autodidacta/

[8] https://www.cyberseek.org/index.html#aboutit

como lo explican los "mandamientos de seguridad que debe tener presente en su trabajo un SYSADMIN"[9]. Si bien en muchas ofertas de trabajo no es requisito fundamental contar con un título de grado para ocupar la posición de administración de redes, Cyberseek indica que es recomendable una licenciatura en ciencias de la computación. Las personas que carecen del título universitario, pero están interesadas en seguir estas carreras pueden hacerlo completando varias certificaciones ofrecidas por organizaciones certificadas. Los administradores de sistemas son responsables de la configuración, mantenimiento, operación y seguridad de los sistemas informáticos y servidores, solucionar problemas y brindar apoyo a otros empleados. Para una transición a la ciberseguridad se deben acreditar en sistemas y seguridad de la información, seguridad de redes y operaciones de seguridad.

Incident Responder. Quienes ocupan la posición de respuesta ante incidentes de seguridad son responsables de investigar, analizar y responder a los ciberataques o incidentes cibernéticos. Sin embargo, su posición no solo es reactiva, sino que también deben monitorear activamente los sistemas y redes para detectar intrusiones, realizar auditorías de seguridad y desarrollar planes de respuestas, así como conocer los planes de continuidad del negocio de la empresa si se produce un ataque exitoso. Una vez finalizado un ataque, quien ocupe esta posición también debe ser capaz de redactar un reporte acerca del incidente en el que se explique con detalle cómo ocurrió el ataque y qué medidas se pueden adoptar para evitarlo. Entre las principales habilidades y conocimientos solicitados para esta posición se requiere conocimiento de LINUX, UNIX, seguridad de redes, sistemas de información y gestión de proyectos.

Analista Forense Digital. Los especialistas en informática forense pueden describirse como los detectives del ciberespacio. Son los responsables de investigar diversas violaciones de datos e incidentes de seguridad, recuperar y examinar datos almacenados en dispositivos electrónicos y reconstruir sistemas dañados para recuperar datos perdidos. También se espera que ayuden a las autoridades a evaluar la credibilidad de los datos y proporcionen asesoramiento experto a los abogados cuando se utilicen pruebas electrónicas en un caso legal. Para esta posición es necesario contar con una licenciatura en ciberseguridad o informática, siendo muy valorado tener además una maestría en informática forense.

Pentester. Son la antítesis de los hackers de sombrero negro. La labor principal de quienes se dedican a realizar pruebas de penetración es analizar sistemas y encontrar vulnerabilidades que puedan explotarse para obtener acceso a los sistemas informáticos. Sin

[9] https://www.welivesecurity.com/la-es/2010/07/30/10-mandamientos-seguridad-sysadmin/

embargo, lo que los distingue de un criminal es que lo hacen legalmente para identificar las debilidades que deben solucionarse y las fortalezas que deben mantenerse. El Pentester es un rol de nivel medio y requiere sólidos conocimientos en seguridad de la información, como también conocimiento de una variedad de lenguajes de programación. Estos perfiles pueden complementar su tiempo laboral dedicándose al hacking ético[10].

Ingeniero en Ciberseguridad. La razón por la que este puesto se menciona casi al final es debido a que es el más avanzado y requiere al menos una licenciatura en informática o en seguridad y el profesional debe tener un alto nivel de competencia en detección, análisis y protección de amenazas. Los ingenieros deben ser creativos y técnicos, ya que algunas de sus responsabilidades incluyen la creación de procesos que resuelvan problemas de seguridad en la producción, la realización de pruebas de vulnerabilidad e incluso el desarrollo de scripts de automatización que ayudarán a manejar y rastrear incidentes. También son responsables de configurar, instalar y mantener los sistemas de seguridad y detección de intrusiones. Además de los mencionados, existen otros perfiles importantes dentro del ámbito de la ciberseguridad como el Threat Hunter, Malware Analyst, entre otros tantos.

En Francia la consideración de puestos por sector para la ciberdefensa es un tema de definición de recurso humanos, tema que manejan y lo definen las Direcciones de Recursos Humanos. El país cuenta con una Dirección de Recursos Humanos a nivel Ministerial y en cada una de las Fuerzas. El COMCIBER y el Agrupamiento Ciber es un comando o agrupamiento conjunto, por ello cada Dirección de Recursos Humanos de cada Fuerza puede ser o es solicitada para encontrar las personas apropiadas para los puestos requeridos por el COMCIBER. De todos modos, es un tema sobre el cual Francia mantiene reservas y explícitamente no quiere hablar del tema.

Israel tiene un centro de ciberdefensa y este tiene la responsabilidad de defender todos los sitios estratégicos del país –comenta nuestra el entrevistado- entonces definir los puestos para cada sector o competencia de la ciberdefensa es un tema de estrategia. Esto se puede ver o sucede en el Ejército y también en otras organizaciones de defensa en Israel, pero siempre la oficina de inteligencia es la misma para todos; no existe eso de que una agencia tiene una inteligencia y otra no sabe lo que ella sabe. Cada agencia o Fuerza tiene su responsabilidad y su centro o cuerpo ciber pero la inteligencia es la misma para todos, esto es algo muy pero muy importante –remarca la fuente consultada-. Entonces, para defender a nivel nacional hay un ciber nacional, luego cada unidad de defensa, el Ejército y todas las Fuerzas Armadas,

[10] https://www.welivesecurity.com/la-es/2020/01/21/bug-bounty-como-funciona-hacking-etico-caceria-vulnerabilidades/

todas las agencias tienen su unidad ciber que hacen protección, inteligencia ciber, cada uno hace su propia defensa o de lo que le compete, pero al final el nivel nacional es el que tiene la responsabilidad nacional en lo ciber. El Ejército por ejemplo tiene una unidad que hace la defensa de los sitios estratégicos del Ejército, pero debajo de esa unidad, cada unidad del ejército hace su propia protección con su propio equipo ciber, y en tema de ciberataque, la responsabilidad la tiene sólo el Ejército.

Perfiles profesionales orientados a la ciberdefensa

En el caso de España, los perfiles orientados a la ciberdefensa que el país piensa tienen que ver con expertos en ciberseguridad e inteligencia artificial, con buenas capacidades interpersonales. Entre estos se encuentran:

Digital Manager. Este profesional diseña, implementa y evalúa la estrategia digital de las empresas, especialmente las de entorno tradicional que estén en fase de transformación digital o que necesiten disponer de un canal de comercialización online. En cuanto a la formación esperada para este perfil, un Digital Manager debe contar con una formación de grado en márketing, publicidad, gestión de empresas o economía, telecomunicaciones, informática o afines. Un máster o posgrado en analítica de datos, e-commerce, diseño o marketing digital. Por experiencia, deberá haber trabajado en puestos de dirección de marketing, projet manager y tener experiencia en gestión de equipos, como también en implantación y migración de soluciones tecnológicas. Entre las competencias esperadas, se halla la planificación estratégica, la capacidad de resolución de problemas, el liderazgo y la toma de decisiones, al igual que habilidades frente a la automatización y orientación a resultados.

Experto en ciberseguridad. Este perfil es el responsable de detectar errores en el manejo de datos que proceden de dentro o de fuera de las empresas, sea cual sea su sector. A su vez, existen diferentes subperfiles: experto en análisis forense, que investiga un incidente y recupera información de un dispositivo, o el hacking ético que pone a prueba la seguridad de los sistemas. De la formación se espera que cuente con un grado en ingeniería informática o de telecomunicaciones; dependiendo de la rama de especialización necesitará también formación específica en gestión de vulnerabilidades, análisis forense o hacking ético. En aptitudes y competencias se valorará su habilidad para resolver problemas, capacidad analítica, creatividad, conocimiento del negocio y disposición para formarse continuamente.

Ingeniero de Inteligencia Artificial. Este profesional comprende el lenguaje de la inteligencia artificial, es decir cómo emular el pensamiento humano a través de las máquinas para predecir comportamientos y la toma de decisiones de las organizaciones, especialmente de aquellas dedicadas a I+D, el análisis de datos y la propia inteligencia artificial. En su formación deberá disponer de un grado en ingeniería en telecomunicaciones o informática y dominar diferentes idiomas. Se requiere que acredite experiencia en el manejo de datos, la carga, transformación y extracción de éstos, demostrar también conocimientos en métricas, reportes y análisis de datos. En cuanto a aptitudes y competencias se le demanda saber trabajar en equipo y poseer capacidad de análisis y resolución de problemas, atención al detalle, comunicación, visión estratégica y de negocio, inquietud técnica.

Abogado especializado en nuevas tecnologías. Es el responsable de asesorar a las compañías o al Estado en los asuntos relacionados con la confección y negociación de contratos y temas legales vinculados a las nuevas tecnologías. Formación de grado en derecho o doble titulación en derecho y administración y/o dirección de empresas, con máster o posgrado en derecho de las nuevas tecnologías y dominio de idiomas. Este perfil deberá disponer de una alta capacidad de análisis, gestión, organización y eficacia, saber trabajar en equipo, contar con buenas aptitudes comunicativas y empatía.

Talent Manager Director. Es el miembro del comité de dirección empresarial que diseña la estrategia global de búsqueda de talento de una empresa, así como la sucesión y el futuro desarrollo de las personas que la componen. Se espera cuente con un grado en psicología, derecho, relaciones laborales o afines y posgrado de especialización en recursos humanos. En cuanto a aptitudes y competencias deberá contar con visión estratégica de su área, capacidad para gestionar el talento, habilidades comunicativas y de toma de decisiones, habilidades para influir y orientar a las personas.

Capacitación del Recurso Humano para la ciberdefensa

En relación con la capacitación de los recursos humanos para la ciberdefensa, España considera que la consecución de una cultura de ciberseguridad o ciberdefensa no es posible a través de acciones de divulgación, aun cuando son necesarias, sino que requiere de una ingente labor formativa especializada que tenga en cuenta en ese proceso de enseñanza aprendizaje a todos los sectores de la sociedad. Se requiere instaurar una cultura de ciberseguridad inserta en una cultura de seguridad y defensa para implicar en ella a toda la sociedad. Resulta necesario analizar previamente, los elementos claves sobre los que cimentar una sólida cultura

de seguridad y defensa y, posteriormente, abordar la capacitación especializada en ciberseguridad, especialmente en el ámbito universitario.

La fuente consultada comenta sobre la importancia estratégica que para España tiene la capacitación de los recursos humanos de la ciberdefensa, apoyándose en el informe del Spanish Cyber Security Institute (SCSI) según el cual

> "el objetivo principal de la ciberseguridad nacional es proporcionar un ciberespacio seguro que garantice la prosperidad social, cultural y económica de nuestro país, así como las libertades fundamentales de los ciudadanos a través de una cultura basada en la prevención y resiliencia en la que participen, de manera activa e integrada, todos los sectores de la sociedad".

Con relación a este objetivo, el informe del SCSI incluye tres objetivos parciales a alcanzar: un conocimiento de ciber situación fiable y actualizado; mejorar la resiliencia nacional frente a la amenaza cibernética y crear; fomentar una cultura de ciberseguridad. A su vez, vinculado a este tercer objetivo parcial destaca la necesidad de establecer un programa nacional de educación en materia de ciberseguridad, sugiriendo las siguientes acciones: desarrollo de una campaña nacional de ciberconcientización; inclusión en los planes de estudio de todos los niveles educativos (desde primaria hasta post universitarios) de materias relacionadas con el uso responsable de las nuevas tecnologías y específicas en relación con la ciberseguridad; modificación de los programas educativos en las materias relacionadas con ciencia, tecnología e ingeniería; incorporación de materias relacionadas con las nuevas tecnologías y la ciberseguridad tanto en los planes de estudio de las academias militares como en las escuelas de negocio; creación de un programa de centros de excelencia en materia de ciberseguridad; planes de formación y concientización, de carácter obligatorio, destinado a empleados de empresas públicas y privadas. Para esto es necesario plantear políticas de Estado a través de instituciones que se ocupen de desarrollar líneas de acción como: desarrollar un marco de conocimientos de ciberseguridad en los ámbitos técnicos, operativo y jurídico; extender y ampliar programas de capacitación de talento, investigación avanzada en ciberseguridad en cooperación con universidades y centros especializados; impulsar actividades de sensibilización dirigidas a los ciudadanos y empresas sobre cómo proteger mejor su entorno tecnológico; desarrollar programas de concientización en ciberseguridad en colaboración con agentes del sector público y privado; fomentar mecanismos de apoyo a las empresas y profesionales en el uso seguro de las TIC; asesorar y dar soporte al desarrollo de módulos educativos de sensibilización en ciberseguridad, dirigidos a todos los niveles de la enseñanza. Todo esto lleva a cabo en España, la Escuela de Ciberdefensa Nacional.

Además, también atiende la necesaria capacitación especializada que deben recibir otros sectores específicos de la sociedad, para el desarrollo de sus funciones. En tal sentido menciona la necesidad de "potenciar las capacidades militares y de inteligencia para ejercer la respuesta oportuna, legítima y proporcionada en el ciberespacio ante amenazas o agresiones que puedan afectar a la Defensa Nacional". De igual manera se incluye la necesaria capacitación especializada dirigida a profesionales del ámbito jurídico, en relación con el cibercrimen y la ciberdelincuencia, para lo cual se establece como línea de acción:

> "Asegurar a los profesionales del derecho el acceso a la información y a los recursos que les proporcionen el nivel necesario de conocimientos en el ámbito judicial para la mejor aplicación del marco legal y técnico asociado. En este sentido, es especialmente importante la cooperación con el Consejo General del Poder Judicial, la abogacía del Estado, la Fiscalía General del Estado, la Fiscalía Coordinadora de la criminalidad informática y el Consejo General de Abogacía de España".

Para nuestro entrevistado, desde el punto de vista estratégico de España, es evidente que las universidades están llamadas a asumir un protagonismo destacado para el establecimiento de una paulatina cultura de ciberseguridad en sus propias instituciones y desde ellas al resto de la sociedad en su conjunto, con especial incidencia en aquellos sectores especialmente implicados.

La responsabilidad sobre la formación y capacitación, en términos militares, en ciberdefensa recae en el Centro Superior de Estudios de la Defensa Nacional (CESEDEN) y los cursos relativos a la materia son:

Curso básico de ciberdefensa. Es un curso de perfeccionamiento conjunto con carácter informativo. Nace para proporcionar los conocimientos de nivel básico para el desempeño de los contenidos en los puestos relacionados con ciberdefensa en las Fuerzas Armadas y de Seguridad y establecer un nivel de conocimiento común para todo el personal con responsabilidades en este campo. Está dirigido al personal de todos los empleos y niveles, con una duración de cuatro semanas en modalidad a distancia y dos semanas presenciales; se imparte en la Escuela de Especialidades de la Armada "Antonio de Escaño", bajo la dirección de la Escuela Superior de las Fuerzas Armadas y con personal docente del Centro Universitario de la Defensa de Marín.

Curso avanzado de ciberdefensa. Es un curso de perfeccionamiento conjunto de especialización. Su objetivo es proporcionar los conocimientos avanzados en ciberdefensa al

personal de todos los empleos y niveles que se desempeñan en este campo. Consta de dos fases, una a distancia de cuatro semanas y otra presencial de ocho semanas. Se imparte en la Academia de Ingenieros del Ejército de Hoyos de Manzanares, bajo la dirección de la Escuela Superior de las Fuerzas Armadas y con personal del Centro Universitario de la Defensa de Zaragoza. Cuenta además con la colaboración de instituciones y organismos relacionados a la ciberdefensa, los cuales imparten conferencias en el curso.

Curso de administrador de ciberdefensa. Su objetivo es proporcionar los conocimientos necesarios para administradores de seguridad de las TIC, que incluyan tanto la administración de redes como la de sistemas. Está definido como curso de perfeccionamiento conjunto de especialización y está dirigido al personal de todos los empleos y niveles vinculados a este campo. Consta de una única fase presencial de cuatro semanas. Se imparte en la Escuela Técnica de Mando Control y Telecomunicaciones del Ejército del Aire, bajo la dirección de la Escuela Superior de las Fuerzas Armadas y con personal docente del Centro Universitario de la Defensa de Marín.

Curso de análisis forense de ciberdefensa. La necesidad de formar a personal con capacidad para extraer, preservar e interpretar evidencias obtenidas de incidentes en la red es el origen de este curso, definido como curso de perfeccionamiento conjunto informativo y está dirigido al personal de todos los empleos y niveles. Se desarrolla en la Escuela Técnica de Mando Contro y Telecomunicaciones del Ejército del Aire, bajo la dirección de la Escuela Superior de las Fuerzas Armadas y la docencia está a cargo del personal técnico en la materia. Consta de una fase a distancia de cuatro semanas y otra presencial de dos semanas, todas con carácter netamente práctico.

Curso de operador de monitorización de ciberdefensa. Con este curso se forma al personal para dotarlo de la capacidad para comprobar el estado de los sistemas bajo su supervisión, controlando los eventos. Está dirigido al personal de todos los empleos y niveles con conocimientos y formación previa en este campo y es un curso de perfeccionamiento conjunto formativo. Bajo la dirección de la Escuela Superior de las Fuerzas Armadas, se desarrolla en la Escuela de Técnicas de Mando Control y Telecomunicaciones del Ejército del Aire, impartido por personal técnico en la materia. Consta de una fase a Distancia de cuatro semanas y otra presencial de dos semanas, con carácter práctico.

Francia en 2014 crea un Centro de Excelencia en Ciberdefensa, pero no hay mucha información porque es un tema confidencial, nos dice la fuente consultada. Si bien no es un centro militar, no está creado por el Ministerio de Defensa, Francia tiene una manera de ver

la ciberdefensa que es global, con coordinación entre los diferentes ministerios, donde el objetivo es apoyar las empresas que trabajan en este medio y también favorecer el crecimiento de nuevos recursos. En este Centro de Excelencia se forma y capacita al personal cuyo destino es el COMCIBER. El país tiene como objetivo contar con 4.500 efectivos formados en el tema, integrando el COMCIBER en 2025, establecido por la Ley de Programación. Francia trabaja con el principio de Polos de Competencias, donde un Polo de Competencias agrupa en un mismo lugar el conocimiento, la experiencia y el trabajo de expertos que pueden ser empresas, universidades o público en general, referidos a un campo o tema. Este Centro de Formación no es una universidad, no es una empresa, es más un lugar de reflexión para promover el crecimiento de empresas y conocimientos que podrían constituir una base industrial y tecnológica en el área ciber. Ante la consulta si es posible contactar con este Centro de Excelencia en Ciberdefensa, la fuente consultada afirma que Francia no puede o no quiere cooperar en determinados sectores, ámbitos o temas, como por ejemplo en lo relativo a sus fuerzas especiales; por lo tanto, al ser confidencial todo lo relativo a este Centro de Excelencia no sabe cuál es el nivel de apertura que el país puede brindar.

El entrevistado sí hace referencia a definiciones públicas realizadas por el actual comandante Ciber de Francia (en 2021). Desde la perspectiva de quien conduce militarmente el tema ciber en el país, el ámbito ciber está en construcción y por ello se propone una hoja de ruta para su mandato que contempla lo siguiente: 1- mantener una cartografía centralizada de todas las formaciones ciber que puedan beneficiar al Ministerio de Defensa. “El agrupamiento ciber es tan joven, que necesitamos construir esta cartografía, me imagino que en dos años ya estará todo preparado, también que en las diferentes universidades están apareciendo masters y formaciones para participar en ese esfuerzo de guerra ciber”, comenta. 2-participar en la preparación operacional del tema. 3-organizar ejercicios de Estados Mayores, Direcciones y Servicios de ciberdefensa a nivel nacional e internacional. 4-adiestrar y controlar la cadena de lucha informática de defensa de los Estados Mayores. 5-contribuir al adiestramiento de los reservistas operacionales de ciberdefensa del COMCIBER. En Francia hay dos tipos de reservistas, los militares que culminan su carrera y se retiran y pueden servir en los Estados Mayores porque conocen el trabajo desde hace treinta años; y la reserva ciudadana que son jóvenes que no tienen nada que ver con la carrera militar pero que quieren servir a la Defensa y son empleados por competencias, capacidades particulares o interés del Ministerio o las Fuerzas.

En el caso de Israel, “lo que puedo decirte, porque hay mucho que no puedo” (comenta la fuente consultada), “es que tenemos muy buena colaboración en cuanto a formación con unos seis países sobre temas de inteligencia y ciber”. Para Israel, la geopolítica y todas sus

implicancias son muy importantes para colaborar en la información y entender mejor el área global de lo ciber y para eso es necesaria mucha colaboración, debe haber necesariamente mucha colaboración que por otra parte no surge espontáneamente, se deben construir los canales de comunicación, vínculo y confianza para que luego haya intercambios tanto a nivel profesional como de tipo educativo en todo sentido. "Hay países que me dicen: yo quiero saber cómo atacar; y yo les digo: no vas a poder saber cómo hacer el ataque si antes no sabes cómo hacer inteligencia, cómo defender, qué tienes, que te falta…" comenta el entrevistado; de igual manera opina que en su experiencia sólo cuando sabes hacer inteligencia, sabes cómo defender, y cuando sabes cómo defender puedes aprender cómo atacar, cuando sabes cómo atacar puedes hacer o planificar el ataque. "Antes de no saber hacer inteligencia, de no saber cómo defender, no puedes hacer un arma ciber, porque el armamento ciber sólo lo puedes hacer después que entiendas bien el área, después de tener la experiencia. Israel tiene la experiencia, este es su beneficio".

Reclutamiento para la ciberdefensa

Para España el recurso humano para la ciberdefensa es fundamental. "Sería un error estratégico no concederle la importancia que hoy en día tiene" comenta nuestro entrevistado. El país es consciente que las administraciones públicas y, las empresas públicas y privadas, están buscando personal para incorporarlo a sus divisiones de ciberseguridad o ciberdefensa; como también que los últimos estudios e informes globales dan cuenta de un faltante cercano a los tres millones de especialista en ciberseguridad en todo el mundo. "Todo esto explica la importancia del reclutamiento, donde no alcanza con tener veinte o cincuenta personas con perfiles y/o conocimientos generales y experiencia altamente específicas para cada demanda ciber" dice la fuente consultada. En España el reclutamiento militar para la ciberdefensa, para el Mando Conjunto del Ciberespacio, se hace de forma reglamentada mediante la publicación de vacantes con los perfiles adecuados según las necesidades (conocimientos y experiencias en informática, telecomunicaciones y ciberdefensa). En el ámbito civil son las propias empresas las que reclutan al personal o empresas especializadas en recursos humanos quienes lo hacen por encargo. Hay una carrera feroz, una gran competencia real en todo este tema, la formación y el reclutamiento del personal (altamente escaso) para los puestos de ciberseguridad y ciberdefensa.

"Nosotros entendemos o pensamos que estamos avanzando muy bien en este tema ciber, somos uno de los países fuerte en el tema" manifiesta la fuente israelí. Para ellos, todo empieza abajo, con los niños, entonces "si no van a tener escuelas particulares de ciberdefensa, computadoras, acceso a la tecnología, profesores con conocimiento que los formen, entonces

la gente no va a llegar con un conocimiento básico para poder apoyar en este tema, o desarrollar lo que necesitan las unidades ciber". "Si yo como experto, como político, como militar, quiero saber la capacidad de reclutamiento y formación que tiene un país, lo primero que voy a preguntar sobre un país o región es si tienen escuelas, áreas y tecnologías para estudiar esto desde temprana edad".

Para entender el reclutamiento de personal en ciberdefensa en Israel, es necesario primero entender que en el país cada hombre y mujer que termina el colegio secundario pasa por el ejército (sin excepciones). Por esto, para ellos es muy fácil contar con información sobre los posibles candidatos a reclutar, porque a los 15 o 16 años, dos años antes de finalizar el colegio, empiezan con cursos sobre áreas ciber y luego hacen exámenes sobre estos temas; y porque cuando ingresan al Ejército, todos quieren llegar a estas unidades ciber. En este sentido, primero cuentan fácilmente con información útil para la oficina de recursos humanos, luego todos los años los candidatos o los interesados hacen exámenes de todo tipo, incluso algunos muy particulares, preparados por las unidades ciber. Entonces, "el beneficio que tiene Israel es que el Ejército de Israel es el Ejército del pueblo y toda su población pasa por él antes de pasar por la vida civil" comenta el entrevistado.

Israel al igual que todos, debe enfrentar las dificultades que presenta retener al personal en áreas altamente especializadas, y el área ciber no es la excepción. Para el país pensar soluciones para retener el personal es un tema muy importante porque hay mucha competencia y por lo mismo, el personal se mueve hacia donde más beneficios obtiene. Un soldado con edades entre veintiuno a veintitrés está recién saliendo a desarrollar su carrera al mundo civil, sale a estudiar, a trabajar y tiene la posibilidad de ganar más dinero que en el Ejército. Frente a esta realidad, Israel se ve obligado a planificar específicamente para retener el personal en esta área. Lo que hacen –explica la fuente consultada- es ofrecer beneficios que puede ser dinero, posibilidades de estudiar, salidas y otras posibilidades. "Hay beneficios para el área ciber que no tienen el resto de las áreas" el entrevistado explica que ésta es una línea de estrategia muy interesante para tener en cuenta.

Conclusiones

En Argentina, por diferentes motivos, se evidencia una seria dificultad para encontrar referencias sólidas y exhaustivas que den cuenta de la producción académica y estados del arte sobre los temas ciber investigados, en particular con la mirada puesta en lo social, en los actores, en los procesos, en las estructuras y no en lo técnico informático. Sin embargo, en los alcances de esta investigación no podemos afirmar que dicha producción no exista o sea

escasa. Conocer qué leen y cuáles son las fuentes técnicas e intelectuales, de determinadas comunidades y sus actores, es de fundamental importancia para determinar los marcos teóricos-conceptuales que orientan decisiones y estrategias; éstas luego se plasman en acciones tanto en los ámbitos académicos, operativos y políticos, que acercan o alejan a dichos actores y sus comunidades, internamente a nivel país, pero también hacia afuera. Creo que hay que hacer un esfuerzo mayor en disponer de relevamientos de bibliografía especializada en la temática y que los mismos circulen pública y libremente en el mundo académico, es decir que se publiquen, sean consultadas y citadas en trabajos de investigación, reportes e informes tanto políticos, técnicos y académicos.

Paz en el quinto dominio. Desde la perspectiva de España, Francia e Israel, de acuerdo con los entrevistados, todos los países están enfrentados o combaten en el ciberespacio, dado que ahora se combate aún sin tener guerras declaradas y sin los parámetros y condiciones de las guerras tradicionales. En este contexto es que los países se enfrentan a los robos masivos de información en temas de Defensa Nacional, datos personales, económicos y financieros, de investigaciones científicas, públicos y privados, ataques directos a objetivos estratégicos, a infraestructuras críticas. Todos estos objetivos pueden ser alterados, atacados, espiados, denegados; y donde de todo eso, sólo entre el 15 y 20 por ciento, son ataques dirigidos por Estados. Es en este sentido y contexto que el ciberespacio adquiere una gran relevancia desde el punto de vista tanto para atacar como para defender.

Pensar la paz en el quinto dominio, no es pensar que todo lo anterior no exista o que los actores se transformarán en ingenuos, amigables y honorables. Pensar la paz en el quinto dominio, es pensar de qué manera se resguardan los intereses nacionales de todos los posibles incidentes mencionados, de qué manera se neutralizan o minimizan las amenazas potenciales o reales que enfrenta una nación en este ámbito.

De acuerdo con esta investigación, una cuestión básica para pensar la paz en el quinto domino es conocer, focalizar y dominar tres temas: la ciberdefensa, el ciberataque y la ciberinteligencia. Ciberdefensa, es decir cómo se hace seguridad para los intereses nacionales y todos los modos estratégicos para lograrlo. Ciberataque, conlleva conocer debilidades, estrategias y desarrollar capacidades, entendiendo que pasa en el entorno de los objetivos estratégicos a proteger, en el de los potenciales atacantes, comprendiendo desde la expertiz técnica qué se necesita hacer para defender y, hacer todo lo que se necesita hacer para ello. Finalmente la ciberinteligencia debe estar puesta al servicio de todos los ámbitos y sectores a proteger o de interés nacional (social, económico, militar, estratégico…), debe servir para que el Estado, sus decisores políticos y mandos operacionales entiendan los riesgos, las

oportunidades, qué necesitan conocer del adentro y del afuera en cada situación u objetivo estratégico; saber cuándo y cómo se debe atacar o defender, si se lo puede hacer; y en caso que no, que daños a corto, mediano y largo plazo conllevarán. Pensar la paz en el quinto dominio es más que sólo un pensamiento ingenuo, o una expresión de buenos deseos, debe ser un pensamiento estratégico a largo plazo de políticas, acciones e inversiones.

Si la Paz en el quinto dominio requiere pensar en la ciberdefensa, el ciberataque y la ciberinteligencia, las cuales son áreas con requerimientos técnicos altamente especializados y escasos, pensar en los recursos humanos adquiere una importancia estratégica real y actual; entendiendo además que es de los temas más importantes dentro de lo ciber para aquellos países que denotan un liderazgo en el área. Por ello España, Francia e Israel consideran que es prioritario, estratégicamente hablando, saber cómo se piensan, se definen y se implementan todos los aspectos relativos a los recursos humanos (formación, reclutamiento, puestos, niveles y requerimientos de expertiz, retención, entre otros). Es tan importante pensar los recursos humanos que Israel lo implementa desde que la población tiene 16 años y España lo declaró un bien estratégico a defender.

En Francia la consideración de puestos por sector para la ciberdefensa es un tema de definición de recursos humanos, tema que manejan y definen las Direcciones de Recursos Humanos de cada Fuerza según los requerimientos del COMCIBER para los puestos a cubrir. Sin embargo, es de tal importancia estratégica que es un tema sobre el cual Francia mantiene reservas y explícitamente no habla. En el caso de Israel, este país tiene un centro de ciberdefensa cuya responsabilidad es defender todos los sitios estratégicos del país, entonces definir los puestos para cada sector o competencia de la ciberdefensa es un tema de estrategia. Para defender a nivel nacional hay un ciber nacional, luego cada unidad de defensa, el Ejército y todas las Fuerzas Armadas y, todas las agencias del país tienen su unidad ciber, que hacen protección, ciberinteligencia y su propia defensa en lo que les compete. En este marco, algunos de los puestos mencionados fueron: *Administrador de Sistemas, Incident Responder, Analista Forense Digital, Pentester, Ingeniero en Ciberseguridad*. En el caso de España, los perfiles orientados a la ciberdefensa que el país piensa tienen que ver con expertos en ciberseguridad e inteligencia artificial, con buenas capacidades interpersonales; entre estos se encuentran: *Digital Manager*, *Experto en ciberseguridad*, *Ingeniero de Inteligencia Artificial*, *Abogado especializado en nuevas tecnologías* y *Talent Manager Director*, entre otros.

Desde el punto de vista de España, la capacitación del recurso humano para la ciberdefensa, no es posible a través de acciones de divulgación, aun cuando éstas son necesarias, sino que requiere de una colosal labor formativa especializada, que tenga en cuenta

en ese proceso de enseñanza aprendizaje a todos los sectores de la sociedad. En este sentido se mencionan como objetivos a alcanzar: un conocimiento de ciber situación fiable y actualizado; mejorar la resiliencia nacional frente a la amenaza cibernética y crear, fomentar una cultura de ciberseguridad. Para el último se sugieren las siguientes acciones: desarrollo de una campaña nacional de ciberconcientización; inclusión en los planes de estudio de todos los niveles educativos de materias relacionadas con el uso responsable de las nuevas tecnologías y creación de un programa de centros de excelencia en materia de ciberseguridad; planes de formación y concientización, de carácter obligatorio, destinado a empleados de empresas públicas y privadas.

Para esto, en la visión de los países objetos de este estudio, es necesario plantear políticas de Estado a través de instituciones que se ocupen de desarrollar líneas de acción como: desarrollar un marco de conocimientos de ciberseguridad en los ámbitos técnicos, operativo y jurídico; extender y ampliar programas de capacitación de talento, investigación avanzada en ciberseguridad en cooperación con universidades y centros especializados; impulsar actividades de sensibilización dirigidas a los ciudadanos y empresas sobre cómo proteger mejor su entorno tecnológico; asesorar y dar soporte al desarrollo de módulos educativos de sensibilización en ciberseguridad, dirigidos a todos los niveles de la enseñanza.

En España, todo esto está a cargo de la Escuela de Ciberdefensa Nacional. Así responsabilidad sobre la formación y capacitación, en términos militares, en ciberdefensa recae en el Centro Superior de Estudios de la Defensa Nacional (CESEDEN) y los cursos relativos a la materia son: *Curso básico de ciberdefensa*, *Curso avanzado de ciberdefensa*, *Curso de administrador de ciberdefensa*, *Curso de análisis forense de ciberdefensa*, y *Curso de operador de monitorización de ciberdefensa*.

Francia en 2014 crea un Centro de Excelencia en Ciberdefensa, pero no hay mucha información porque es un tema confidencial; sin embargo, podemos decir que tiene una manera de ver la ciberdefensa que es global, con coordinación entre los diferentes ministerios, donde el objetivo es apoyar las empresas que trabajan en este medio y también favorecer el crecimiento de nuevos recursos. En este Centro de Excelencia se forma y capacita al personal cuyo destino es el COMCIBER. El país tiene como objetivo contar con 4.500 efectivos formados en el tema, integrando el COMCIBER en 2025, establecido por la Ley.

Desde la perspectiva de quien conduce militarmente el tema ciber en Francia, el ámbito ciber estaba en construcción (en 2021) y por ello se proponía una hoja de ruta para su mandato que contempló lo siguiente: 1- mantener una cartografía centralizada de todas las

formaciones ciber que puedan beneficiar al Ministerio de Defensa. 2-participar en la preparación operacional del tema. 3-organizar ejercicios de Estados Mayores, Direcciones y Servicios de ciberdefensa a nivel nacional e internacional. 4-adiestrar y controlar la cadena de lucha informática de defensa de los Estados Mayores. 5-contribuir al adiestramiento de los reservistas operacionales de ciberdefensa del COMCIBER.

En el caso de Israel, la geopolítica y todas sus implicancias son muy importantes para colaborar en la información y entender mejor el área global de lo ciber. Para eso es necesaria mucha colaboración, que por otra parte no surge espontáneamente, se deben construir los canales de comunicación, vínculo y confianza para que luego haya intercambios tanto a nivel profesional como de tipo educativo en todo sentido. Así, para el país, la experiencia y cooperación son fundamentales en la formación, y esto implica un esfuerzo estratégico del país, sus agencias y sus agentes para construir vínculos, comunicación y confianza.

Si consideramos que estudios e informes globales dan cuenta acerca de las búsquedas de personal, por parte de las administraciones públicas como también de las empresas públicas y privadas, de donde surge un faltante cercano a los tres millones de especialistas en temas ciber en todo el mundo (para el año 2021); por sí solo esto explica la importancia del reclutamiento para España, y debería explicarlo para todos. Hay una competencia feroz y real en cuanto al reclutamiento (con el componente formación de por medio) de personal para los puestos de ciberdefensa y ciberseguridad. Para este país, no alcanza con tener veinte o cincuenta personas con perfiles y conocimientos generales, es de vital importancia contar con profesionales con conocimientos y experiencias altamente específicas para cada demanda del área, esto implica tiempo, estrategia, políticas consensuadas, capacidades de infraestructura y económica: pero, sobre todo, comprensión real del escenario actual y futuro.

Desde la postura de Israel, en la proyección, planificación y visión del reclutamiento, entra en juego considerar, desde una posición real y no meramente intencional, escuelas de ciberdefensa, computadoras, acceso a la tecnología, profesores con conocimiento real que formen expertos, sin lo cual no se puede llegar a contar con una masa crítica con conocimiento básico para poder apoyar, trabajar o desarrollar lo que necesitan las unidades ciber. Para saber la capacidad de reclutamiento es necesario conocer la capacidad de formación que tiene un país; en esto se halla implicado las políticas educativas en el tema, la existencia y trayectoria de escuelas o ámbitos de formación, el desarrollo del área ciber, la existencia y tipo de tecnologías, los rangos de edad en la que adquieren, desarrolla y especializan los conocimientos, entre otros factores.

En el tema de reclutamiento, pensar soluciones para retener el personal es un tema muy importante para todos los países, debido a la intensa competencia entre reclutadores y en función de que el personal se mueve hacia donde más beneficios obtiene. Frente a esta realidad, algunos países se ven obligados a planificar específicamente acciones para retener al personal en esta área; es decir, la retención no se da por sí sola.

Y el mayor o menor éxito depende de la mayor o menor capacidad de planificar acciones de contención, es por eso por lo que quienes entienden de esta realidad como una necesidad estratégica, ponen gran parte de su esfuerzo en pensar y lograr las mejores acciones (planificadas, consensuadas, no esporádicas, no aisladas, no discontinuas) para contar con el mejor personal posible.

Bibliografía

- Arquilla, J.; Ronfeldt, D. (1993). "Cyberwar is Coming!". En Comparative Strategy, Vol 12, No 2, Spring, pp. 141-165.

- Baños, Pedro (2020). El dominio mental. La geopolítica de la mente. Ed. Ariel, Barcelona.

- Bencsath, B.; Pek, G.; Buttyan, L.; Felegyhazi, M. "The cousins of Stuxnet: Duqu, Flame and Gauss". En Future Internet 2012, No 4, pp. 971-1003. Disponible en http://www.mdpi.com/journal/futureinternet

- Ciberseguridad: ampliación del campo de lucha. https://www.cairn-mundo.info/revista-politique-etrangere-2018-2.htm

- Cobo, Beatriz de León. Las claves para comprender la estrategia cibernética francesa y sus riesgo. https://atalayar.com/content/las-claves-para-comprender-la-estrategia-cibern%C3%A9tica-francesa-y-sus-riesgos

- De Lucca, C. D. (2013). "The Need for International Laws of War to Include Cyber Attacks Involving State and Non-State Actors". En Pace International Law Review, vol. 3:9, enero 2013, pp. 278-315.

- De Tomás Morales, S. y Velázquez Ortiz, A. P. (2013). "La responsabilidad del Mando en la conducción de las operaciones durante la ciberguerra: la necesidad de un adiestramiento eficaz". Premio Defensa 2013, categoría "José Francisco de Quevedo y Lombardero". Disponible en http:// www. portalcultura. mde.es/actividades/ premios/ defensa/2013/

- Escuela de Altos Estudios para la Defensa. Necesidad de una conciencia nacional de ciberseguridad. La ciberdefensa: un reto prioritario. Disponible en https://publicaciones.defensa.gob.es/media/downloadable/files/links/m/o/monografia_ceseden_137.pdf

- Estrategias de Seguridad Cibernética de los Países Bajos, Francia y Alemania. https://www.ccn-cert.cni.es/en/gestion-de-incidentes/lucia/23-noticias/204-estrategias-de-seguridad-cibernetica-de-los-paises-bajos-francia-y-alemania.html

- Fojón Chamorro, Enrique. Formar ciberguerreros. Disponible en https://www.realinstitutoelcano.org/cibers/ciber-elcano-no-24/

- Foltz, A. C. (2012). "Stuxnet, Schmitt Analysis, and the Cyber Use-of-Force Debate". En JFQ, issue 67, 4th quarter 2012, pp. 40-48.

- Gautier, Luis. Ciber: las claves de la defensa y la seguridad de los franceses. en Politique Étrangére, número 2, 2018, pg. 29-42. https://www.cairn.info/revue-politique-etrangere-2018-2-page-29.htm

- Géry, Aude. El derecho internacional y la proliferación de las armas cibernéticas. en Politique Étrangére, número 2, 2018, pg. 43-54. https://www.cairn.info/revue-politique-etrangere-2018-2-page-43.htm

- Gómez de Agreda, Ángel (2021). Mundo Orwel. Manual de supervivencia para un mundo hiperconectado. Barcelona.

- Gomez de Agreda, A. (2012). "El ciberespacio como escenario del conflicto. Identificación de las amenazas. El ciberespacio nuevo escenario de confrontación". Monografías CESEDEN, No. 126, febrero 2012, pp. 169-203.

- González Cussac, J. L. (2010). "Estrategias legales frente a las ciberamenazas. Ciberseguridad, retos y amenazas a la seguridad nacional en el ciberespacio". En Cuadernos de Estrategia, No 149, diciembre 2010, pp. 92-102.

- Hathaway, O. A.; Crootof, R., Levitz, P.; Nix, H.; Nowlan, A.; Perdue, W.; Spiegel, J. (2012). "The law of ciber attack". En Yale Faculty Scholarship Series, paper 3852, 2012, pp. 817-886.

- Hollis, D. B. (2007). "Why States Need an International Law for Information Operations". En 11 Lewis and Clark Rev (1023, 1093, 2207), pp. 1023-1061.

- Ministerio de Defensa. (2013). "Necesidad de una conciencia nacional de ciberseguridad. La ciberdefensa: un reto prioritario". Monografía, No 137, CESEDEN, 2013.

- Ministerio de Defensa (2011). "Ciberseguridad. Retos y amenazas a la seguridad Nacional en el Ciberespacio". En Cuadernos de Estrategia, No 149, Ministerio de Defensa, 2011.

- Nocetti, Julien. Geopolítica de la ciberconflictividad en Politique Étrangére, número 2, 2018, pg. 15-27. https://www.cairn.info/revue-politique-etrangere-2018-2-page-15.htm

- Pastor Acosta, Oscar; Pérez Rodriguez, Antonio; Arnáiz de la Torre, Daniel; Taboso Ballesteros, Pedro. (s d). Seguridad nacional y ciberdefensa.

- Pou Rodriguez, Aina. Demanda en ciberseguridad, sector de pleno empleo. Disponible en https://cybersecuritynews.es/demanda-en-ciberseguridad-sector-de-pleno-empleo/

- Raboin, B. (2013). "Corresponding Evolution: International Law and the Emergence of Cyber Warfare". En Cleveland State Law Review, No 31, 2013, pp. 603-668.

- Schmitt, M. N. y otros (2013). Manual on the International Law Applicable to Cyber Warfare. Cambridge University Press, 2013.

- Schmitt, M. N. (2011). "Cyber operations and the jus ad bellum revisited". En Villanova Law Review, vol. 56, diciembre 2011, pp. 569-606.

- Tikke, E. (2010). International Cyberincidents. Legal considerations, CCDCOE, 2010.

- Tikke, E. y otros (2008). Cyber Attacks Against Georgia: Legal Lessons Identified, CCDCOE, 2008.

- Ziolkowski, K. (2012). "Ius ad bellum in Cyberspace-Some Thoughts on the "Schmitt-Criteria" for Usse of Force". En CZOSSECK, C., 2012 4th Iternational Conference on Cyber Conflict, NATO CCD COE Publications, Tallinn, 2012.