Creación del Comando Operacional de Ciberdefensa

El Estado debe tener la capacidad de Ciberdefensa, ante posibles ciberataques a la nación y sus activos críticos, para estar en la capacidad de neutralizarlas, a fin de proteger sus intereses nacionales. El Comando Conjunto tiene como una de sus funciones, garantizar a través de las Fuerzas Armadas, la soberanía e integridad territorial, siendo el ciberespacio el nuevo escenario en el cual se desarrollan los ciberataques a un Estado.

Coronel FAP
Daniel Iván
Taipe Domínguez

Ingeniero de Sistemas con certificaciones internacionales vigentes en CEH, ECSA, CEI e ITIL. Diplomado en Técnicas de Antihacking en España y Diplomado de Administración en IAAFA, en Texas. Ha participado en el Foro de Líderes de Seguridad, Cartagena; Operation Informations Regional, USSOUTHCOM, Miami; Security Conference, Las Vegas; UK Defense & Security, Londres; Ciberseguridad, Chicago; Information Security, Bogotá; Forum international de la Cibersécurité, Francia; y recientemente en el curso de Desarrollo de Políticas de Ciberseguridad por la Universidad Nacional de Defensa en Washington D.C. Actualmente es Jefe de Ciberdefensa del Comando Conjunto de las Fuerzas Armadas del Perú. Docente en la Escuela Conjunta de las Fuerzas Armadas, Docente del Diplomado Internacional de Ciberseguridad del CAEN y Expositor en eventos de Ciberseguridad y Ciberdefensa.

Con fecha 13 de Junio del presente año, el Jefe del Comando Conjunto de las Fuerzas Armadas del Perú, ha aprobado la incorporación dentro de la organización del Comando Conjunto,[1] un órgano de ejecución de operaciones en el ámbito del ciberespacio; denominado COMANDO OPERACIONAL DE CIBERDEFENSA (COCID), el cual tendrá la siguiente misión y organización:

Su misión será la de planear, organizar y dirigir operaciones conjuntas de carácter defensivo (Ciberdefensa), integradas por personal calificado en operaciones informáticas, debidamente equipado y entrenado para neutralizar ciberataques sobre nuestras fuerzas y medios de alto valor militar, político y/o económico, impidiendo el daño a nivel estratégico, operacional o táctico.

Las fuerzas asignadas estarán conformadas por el personal y medios de las unidades de Operaciones Informáticas (Cibercomandos), así como otras fuerzas de las Instituciones Armadas que, producto del planeamiento operacional conjunto, resulten necesarias; asignación que se hará efectiva para la ejecución de los planes de operaciones estratégicos correspondientes.

El Estado Mayor Conjunto estará constituido por personal del Ejército, Fuerza Aérea y Marina de Guerra del Perú.

En permanente articulación con las Fuerzas Armadas, por intermedio del Jefe del Comando Conjunto, se solicitará a los institutos, personal capacitado para integrar el Cibercomando Conjunto y se coordinará las tareas a realizar en cada Cibercomando de las Fuerzas Armadas.

El Comando Operacional de Ciberdefensa, dependerá del Comando Conjunto y articulará con los Cibercomandos de cada Fuerza Armada.

PALABRAS CLAVE: Comando Conjunto, Fuerzas Armadas, ciberespacio, cibercomando, ciberdefensa, Comando Operacional, ciberataque, cibernética.

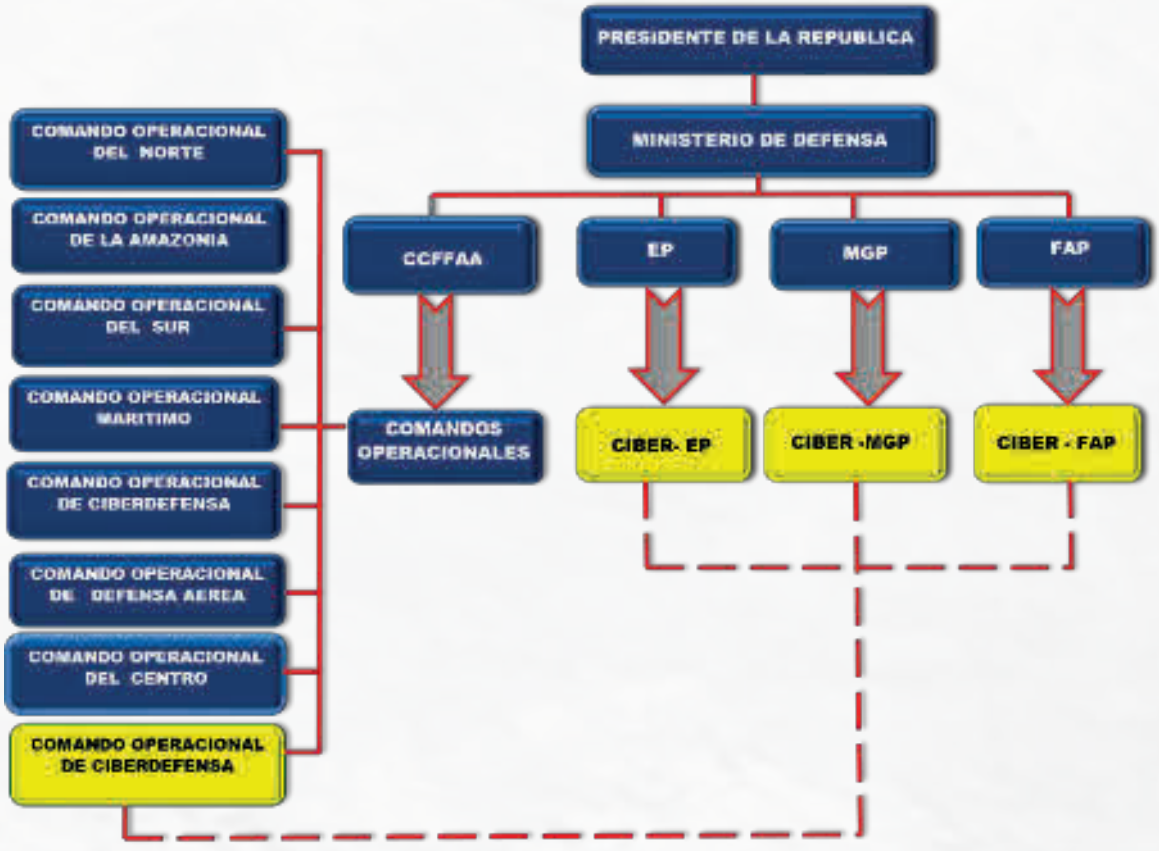
Fuente: Coronel FAP Daniel Taipe Dominguez.[2]

Actualmente, ya se encuentra creado como parte de la Organización, lo que se requiere ahora son los recursos financieros para su implementación (Hardware, software, Instrucción) y para ello nos hemos auto impuesto la tarea de realizar un Proyecto de Inversión Pública (PIP), el cual se encuentra en la etapa final.

CIBERATAQUES AL ESTADO Y A ACTIVOS CRÍTICOS

Actualmente los ciberataques suceden todos los días, la mayoría están orientados al robo de información que se puede convertir en dinero, no interesa de donde se obtenga o el efecto que cause, el objetivo es uno solo: dinero.

El ataque puede ser a una Instalación Militar para robar información confidencial que le pueda servir a otro país y eso es dinero, como lo sucedido a EEUU, en que china roba los planos del Avión de caza F-35 y El Director de la Inteligencia Nacional de Estados Unidos, James Clapper, lo toma como un ciberataque a los activos críticos militares y advierte de un ataque cibernético “a gran escala” podría “debilitar toda la infraestructura del país norteamericano; “En mis más de 50 años en el negocio de la inteligencia, no recuerdo un momento en el que hemos estado acosados por una mayor variedad de desafíos y ries-



Fuente: Coronel FAP Daniel Taipe Dominguez.

CUADRO COMPARATIVO SOBRE LAS CAPACIDADES EN CIBERDEFENSA

Fuente: Observatorio de la Ciberseguridad en América Latina y el Caribe.

gos de todo el mundo, tanto a nivel regional como funcionalmente", afirmó Clapper ante el Comité de Inteligencia de la Cámara de Representantes.

El Jefe de Inteligencia advirtió a los legisladores que el espionaje cibernético contra el país probablemente aumentará, en parte porque los hackers se enfrentan a poco o a ningún castigo y que este tipo de amenazas "a la seguridad nacional y económica están aumentando en frecuencia, en escala, en sofisticación y gravedad del impacto".

La Casa Blanca acusa a China de estar detrás del hackeo de información federal de sus trabajadores, detectado en abril pero cometido en diciembre del año pasado, que comprometió los datos personales de unos 22 millones de empleados que trabaja o trabajaba para el Gobierno.

Pekín, sin embargo, califica las acusaciones de ataque cibernético de Washington de contraproducentes e hipócritas, ya que las fugas de inteligencia han revelado que el propio Estados Unidos es el autor más activo de espionaje cibernético contra los países extranjeros, especialmente contra China.

Estas afirmaciones entre esos dos países, nos demuestra que esta nueva forma de hacer la guerra o los ciberataques, hacen que se desconozca al enemigo, no hay evidencias concretas que el ataque pudo haber venido de tal país, porque es anónimo, también es muy económica ya que no se gasta material en dicho ataque, no se exponen vidas humanas, ya que lo hacen desde su oficina tomándose un café, y sobre todo que el efecto que causa un ciberataque bien dirigido puede causar más daño a la economía de un país que un misil.

Diariamente los hackers perfeccionan sus habilidades, crean nuevas herramientas para vulnerar la seguridad informática, y casi siempre lo logran, hay un dicho de autor anónimo en Ciberseguridad que dice "El hacker debe tener suerte solo una vez para irrumpir en los sistemas, el Administrador en cambio debe de tener suerte siempre para que no lo logren", esto se comprueba con los miles de ciberataques que se realizan en todo el mundo.[3]

Asimismo, la Organización de Estados Americanos (OEA), realiza constantemente estudios e informes sobre el estado actual de muchos aspectos entre los cuales se encuentra la Ciberdefensa, en el informe denominado "OBSERVATORIO DE LA CIBERSEGURIDAD EN AMÉRICA LATINA Y EL CARIBE", el estado actual de dicha capacidad en los diferentes países, aquí se ha hecho un extracto del informe que

nos permite conocer el grado de madurez de la Ciberseguridad en estos países.

DEFENSA CIBERNÉTICA

Puede haber eventos que repercuten en los intereses de seguridad nacional relacionados con la seguridad de la red, la capacidad de recuperación cibernética, la respuesta a incidentes y el intercambio de información, que requieren la participación de los ministerios y organismos de defensa. Por lo tanto, se necesita la preparación de una estrategia que coordine a todas las organizaciones participantes para garantizar un enfoque integrado para hacerle frente a las amenazas a la seguridad nacional. Esta evaluación no pretende examinar la capacidad técnica o militar, sino que se centra en los atributos fácilmente observables, tales como planificación estratégica, organización y coordinación.

LEYENDA, SOBRE EL SIGNIFICADO DE LOS NÚMEROS EN CADA PAÍS:

INICIAL (1)

No hay gestión de la defensa cibernética; si es que existe, puede ser distribuida entre las fuerzas armadas y/o algunas otras organizaciones gubernamentales; no hay una estructura de mando clara para la seguridad cibernética en las fuerzas armadas.

FORMATIVO (2)

Las unidades de operación de defensa cibernética se incorporan a las diferentes ramas de las fuerzas armadas, pero no existe una estructura central de mando y control.

ESTABLECIDO (3)

Dentro del ministerio responsable de la defensa, existe una organización definida para enfrentar los conflictos utilizando medios cibernéticos.

ESTRATÉGICO (4)

Se integran a la estrategia de defensa nacional la experticia altamente especializada con capacidades cibernéticas estratégicas avanzadas y conocimiento total de la situación.

DINÁMICO (5)

El ministerio responsable de la defensa contribuye al debate mediante el desarrollo de un entendimiento internacional común del punto en el que un ataque cibernético podría desencadenar una respuesta de varios dominios.

¿POR QUÉ ES IMPORTANTE LA CREACIÓN DE UN CIBERCOMANDO EN LAS FUERZAS ARMADAS?

El Estado debe tener la Capacidad de Ciberdefensa, ante posibles ciberataques a la nación y sus activos críticos, para estar en la capacidad de neutralizar dichas amenazas, a fin para proteger sus intereses nacionales.

El Comando Conjunto tiene como una de sus funciones, garantizar a través de las Fuerzas Armadas, la soberanía e integridad territorial. Siendo el ciberespacio, el nuevo escenario en el cual se desarrollan los ciberataques a un Estado.

Las Fuerzas Armadas, es la responsable en el Estado de tener la capacidad de respuesta ante una agresión externa, sea en cualquiera de los ámbitos (Aéreo, Marítimo, Terrestre, Espacial y Ciberespacio), y el responsable de esta tarea es el Comando Conjunto de las Fuerzas Armadas, es por ello que esta organización de Ciberdefensa, debe ser Conjunta (Fuerza Aérea, Marina de Guerra y Ejercito del Perú), para que en el momento de un conflicto se pueda contar con las capacidades del personal entrenado, así como el *hardware*, *software* de las Fuerzas Armadas y constituirse en una sola fuerza capaz de doblegar dicho ataque, asimismo debe ser una Organización multidisciplinaria, que involucre personal de distintas especialidades y calificaciones, entre las cuales no debe de faltar los especialistas en Informática, quienes dominan el campo tecnológico, las ultimas herramientas de hardware y software, o crear las propias, los especialistas en Inteligencia, que son los que nos brindaran la información de inteligencia propicia para prever un ataque o brindar los objetivos más propicios, así como los expertos en Comunicaciones y Electrónica que es primordial contar con esa capacidad, y de otras especialidades muy importantes, lo cual el conjunto de estas con-

formaran esta nueva organización de Ciberdefensa de las Fuerzas Armadas del Perú.

También es necesario estar en coordinación con la Secretaria de Gobierno Digital y las empresas públicas y privadas a cargo de los activos críticos del Perú, una de ellas que mejor está constituida es la Asociación de Bancos del Perú (ASBANC), para fusionar fuerzas en contra de los Ciberataques.

Estudios realizados por la OEA (Organización de Estados Americanos), indicaron un aumento en el número de ataques contra infraestructuras críticas. Muchas de estas, incluidas las que manejan los sectores financiero, de transporte, de energía y de atención de la salud, dependen de sistemas de control industrial. Muchos de estos sistemas, a su vez, utilizan el internet, lo que les permite a las infraestructuras críticas operar de manera eficiente y barata. Pero por otro lado, la conectividad de los sistemas de control industrial, también les presenta a los delincuentes y terroristas, oportunidades de atacar a países donde se sentirá más.

En América del Sur, solo tres países ya tienen una Política Nacional de Ciberseguridad y casi en su totalidad poseen una Organización de dedicada a la Ciberdefensa (exceptuando a Paraguay, Venezuela, Guyana y Surinam), en el caso de Venezuela y Paraguay están en camino de crear también una Organización de Ciberdefensa.

Se requiere que el Perú concrete la aprobación de la Política Nacional de Ciberseguridad, acerca de la cual se viene trabajando desde hace algunos años, con la participación de los sectores públicos y privados.

Otro aspecto importante que se está impulsando, es la educación del Personal Militar en las Escuelas de Formación y Superiores de las Fuerzas Armadas, en temas de Ciberseguridad, por ser una necesidad. Estamos viviendo la era del Ciberespacio, por lo tanto, tenemos la obligación de estar preparados ante este nuevo escenario.

Como en mi caso, que desde el año 2007, en que tuve la oportunidad de estudiar en el Reino de España sobre Ciberseguridad e inicié una campaña para incentivar la Ciberseguridad en la Fuerza Aérea del Perú. Realizando informes de *Ethical hacking* para comprobar la Seguridad Informática existente en la institución.

Posteriormente continué con esta labor en el Comando Conjunto desde el año 2012, labor que debe ser constante con personal dedicado a esta capacidad de Ciberdefensa, es por ello que dedique el esfuerzo en la sustentación para crear e implementar un Cibercomando de las Fuerzas Armadas.

Como Jefe de Ciberdefensa del Comando Conjunto, desde que cree este Departamento cuando llegue al Comando Conjunto, hace 6 años, puedo decir que logré mi objetivo.

Fuente: Coronel FAP Daniel Taipe Dominguez.[4]

Fuente: Steve Sack, caricaturista. Publicado en http://www.startribune.com/sack-cartoon-russian-hacking/393631531/.

CITAS BIBLIOGRAFICAS

1. Aprobado con Hoja de Recomendación Nro. 002 EMCFFAA/D8/DOCD de fecha 13 de junio del 2017, firmada por el Sr. Almirante, Jefe del Comando Conjunto y Visada por el Sr. Jefe del Estado Mayor Conjunto de las Fuerzas Armadas.
2. Proyecto del logo del Cibercomando de las Fuerzas Armadas, el cual representa con el escudo la Ciberdefensa para proteger los Activos Críticos y la espada representa la ofensiva, solo ante la reacción de un ciberataque.
3. En esta Página Web se encuentran los últimos Ciberataques que ocurren día tras día, https://elpais.com/tag/ataques_informaticos/a
4. Relación de los países que ya cuentan con una organización dedicada a la Ciberdefensa y algunos de ellos que ya tienen también una Política nacional de Ciberseguridad.

BIBLIOGRAFIA

- Política Nacional de Seguridad Digital de Colombia, https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf
- Ciberdefesa e Cibersegurança do Brasil, http://www.asociacioncolegiosdefensaiberoamericanos.org/acdibero/LibrosReunionesDirectores/LIBRO+XVII+CONFERENCIA+-+CIBERDEFESA+E+CIBEREGURAN%C3%87A+NOVAS+AMEA%C3%87AS+%C3%80+SEGUR....pdf
- Política Nacional de Ciberseguridad de Chile, http://www.ciberseguridad.gob.cl/
- Creación del Comando operacional de Ciberdefensa del Ecuador, http://www.eluniverso.com/noticias/2014/09/09/nota/3805401/ffaa-anuncian-2015-comando-operaciones-ciberdefensa
- Comando de Ciberdefensa de Argentina, http://www.fuerzas-armadas.mil.ar/Dependencias-CIBDEF.aspx
- Centro de Ciberdefensa del Uruguay, http://www.defensa.com/uruguay/centro-ciberdefensa-militar-uruguay
- Centro de Ciberdefensa de Bolivia, http://www.eldeber.com.bo/bolivia/Ejercito-boliviano-crea-centro-de-ciberdefensa-20161223-0076.html
- Informe Ciberseguridad 2016, http://observatoriociberseguridad.com/
- Taipe, D. (2014). ¿Porque es necesario un Cibercomando?; En revista Comando en Acción edición Nº 56. Lima: Comando Conjunto de las Fuerzas Armadas del Peru. http://www.ccffaa.mil.pe/publicaciones/CenA/CenA2014/CenA56_2014.pdf.