

SEGURIDAD DE LAS COMUNICACIONES EN LAS OPERACIONES

Felipe Alberto Mediano Dazarola*

Resumen

La planificación y la ejecución de las operaciones navales nacionales, los entrenamientos conjuntos y la participación en actividades combinadas tienen un factor común; la Seguridad de las Comunicaciones (COMSEC). Gracias a los acuerdos bilaterales entre los Gobiernos de Chile y de los EE.UU., las fuerzas armadas de Chile tienen acceso a tecnologías que les permiten interoperar con estándares de nivel mundial y participar en las grandes ligas, obteniendo prestigio profesional a nivel global y un posicionamiento privilegiado a nivel regional. Pero, ¿qué significa y para qué sirven las COMSEC?, ¿cómo logramos obtener acceso a ellas?, ¿quiénes las planifican y coordinan tras bambalinas?, son algunas de las interrogantes que se resolverán en el presente artículo.

Palabras clave: COMSEC; USSOUTHCOM; EMCO; CCIB; DIRECTELINE.

Las comunicaciones son un elemento vital para el éxito de las operaciones navales, tanto en sus fases de planificación como de ejecución. A su vez, otorgarle seguridad a las comunicaciones permite que la información transmitida entre los mandos mantengan los tres pilares de la seguridad de la información; confidencialidad, integridad y disponibilidad.

La confidencialidad permite que la información sea recibida exclusivamente por los usuarios autorizados por un emisor, evitando que ésta sea divulgada a personal no autorizado. En la institución, este pilar está definido a través de la clasificación de la información en pública, reservada o secreta, así como de la definición de los destinatarios de la información.

La integridad permite que la información sea exactamente lo que el emisor entregó, otorgándole precisión y evitando su modificación por medio del borrado o cambios en la información.

La disponibilidad es aquella que permite a los usuarios contar con la información cuando la necesitan, accediendo a ella por canales autorizados y expeditos, los cuales a su vez deben contar con sistemas que eviten que un agente adversario pueda materializar ataques de denegación de servicios.

A lo largo de la historia, han existido diferentes formas de otorgar seguridad a las comunicaciones, ya sea por medio del uso de técnicas de encriptado (palabra que significa ocultar, derivada del latín y del griego), tablas de códigos, sistemas de cifrado manuales, mecánicos, electro-mecánicos y electrónicos.

En la actualidad, la institución posee diferentes sistemas que proveen de seguridad, diferenciándose entre la seguridad estática a cargo de la Dirección de Telecomunicaciones e Informática y la seguridad dinámica a cargo de la Dirección de Inteligencia, ambas trabajando

* Teniente 1°. Magíster en Tecnologías de la Información de la Universidad Técnica Federico Santa María. (fmediano@armada.cl).



■ Cuartel General del Comando Sur de los EE.UU., Miami, FL.

en equipo para salvaguardar la información y los sistemas que dan soporte al flujo de órdenes a los diferentes mandos de la institución.

Sin embargo, en un mundo globalizado las organizaciones requieren de la interacción con otras instituciones o agencias, nacionales y extranjeras, en las cuales la seguridad de las comunicaciones demanda la mantención de sus tres pilares para el éxito de sus actividades.

La Armada de Chile no se encuentra exenta de esta necesidad, su constante participación en operaciones navales a nivel conjunto y combinado, exigen que las comunicaciones y los sistemas de mando y control posean capacidades de otorgar seguridad con estándares internacionales, los cuales son necesarios de instalar, entrenar, operar, administrar y actualizar constantemente y de la formada adecuada.

¿Qué es COMSEC?, la mirada estadounidense

Tanto en las doctrinas conjuntas de los EE. UU. como en las de la OTAN, se definen las Operaciones de Información o INFO-OPS (sigla por su denominación en inglés *Information Operations*), introduciéndose a través ellas el concepto de la Seguridad de las Operaciones u OPSEC (sigla por su denominación en inglés *Operations Security*).

Derivado a las OPSEC, se identifican la Seguridad Informática o COMPUSEC (sigla por su denominación en inglés *Computer Security*), la Seguridad de la Transmisión o TRANSEC (sigla por su denominación en inglés *Transmission Security*), el Control de las Emisiones o EMCON (sigla por su denominación en inglés *Emission Control*) y la Seguridad de las Comunicaciones o COMSEC (sigla por su denominación en inglés *Communications Security*).

El Gobierno de los EE. UU. define COMSEC como aquellas medidas adoptadas para negar a personas no autorizadas el acceso a la información tramitada por sistemas de telecomunicaciones gubernamentales y que puedan afectar su Seguridad Nacional. Estas medidas de seguridad consideran procedimientos, equipamiento de hardware y software, así como sus respectivos Sistemas de Claves o KEYMAT (sigla por su denominación en inglés *Key Material*) las cuales son generadas y administradas por la Agencia Nacional de Seguridad de ese país (NSA, por su denominación en inglés *National Security Agency*).

El equipamiento COMSEC se encuentra asociado a diferentes sistemas, dentro de los cuales existen los relacionados con las telecomunicaciones, sistemas de mando y control e incluso sistemas de armas, entre los que se destacan:

- Equipamiento de comunicaciones tácticas de voz en los rangos de frecuencia de HF, VHF y UHF.
- Equipamiento CENTRIXS, sigla de su denominación en inglés *Combined Enterprise Regional Information Exchange System*).
- Sistemas de Data Link Tácticos o TDL (sigla de su denominación en inglés *Tactical Data Link*), como son el caso del LINK-11 y LINK-16.
- Sistemas de transferencia electrónica de voz y datos.



■ Séptima reunión del *Command and Control Interoperability Board*, efectuada en la ciudad de Viña del Mar en noviembre del 2017.

- Sistemas de Administración de Claves Electrónicas EKMS (sigla de su denominación en inglés *Electronic Key Management System*).
- Equipamiento de comunicaciones satelitales.
- Sistemas de Posicionamiento Global (GPS) para las trayectorias de vuelo de misiles.
- Sistemas de identificación de plataformas IFF (sigla de su denominación en inglés *Identification Friend or Foe*).

Si bien los sistemas que utilizan COMSEC son certificados por la NSA para las fuerza armadas de ese país, el Gobierno de los EE. UU. aprueba su operación para países miembros de la OTAN, sus aliados u otras naciones amigas (denominadas *Partner Nations*, como es el caso de Chile), los cuales pueden adquirir tecnología y cifradores COMSEC por medio de acuerdos bilaterales y contratos de autorización de uso y compra de dispositivos a través de los casos de FMS (sigla de su denominación en inglés *Foreign Military Sales*).

Relación COMSEC entre los gobiernos de Chile y de los EE.UU.

Los Gobiernos de Chile y EE.UU. mantienen vigente desde septiembre del año 2004 un acuerdo a través del cual se promueve la interoperabilidad de los sistemas de comunicaciones y de mando y

control a nivel táctico, lo que permite mantener la seguridad de la información en actividades combinadas, tanto bilaterales como multinacionales en que participen ambas naciones. Actualmente, ambos Gobiernos son representados por el Estado Mayor Conjunto de Chile (EMCO) y el Comando Sur de los EE. UU. (USSOUTHCOM), cuyo cuartel general se encuentra ubicado en la ciudad de Miami, Florida.

La interacción a través de USSOUTHCOM, como administrador de las cuentas COMSEC de Latinoamérica y el Caribe, permite a las fuerzas armadas de Chile operar permanentemente y entrenarse utilizando sistemas de comunicaciones, y de mando y control seguras del nivel de la OTAN, en beneficio de las actividades conjuntas y combinadas, tramitando periódicamente los KEYMAT que son utilizados en los diferentes sistemas.

Anualmente, los representantes de USSOUTHCOM, el EMCO, las tres ramas de las fuerzas armadas de Chile y de diferentes agencias gubernamentales de los EE.UU. se reúnen para discutir los avances en las materias de interoperabilidad, nuevos desafíos y requerimientos COMSEC derivados de ellos en el Comité de Mando, Control e Interoperabilidad CCIB (sigla de su denominación en inglés *Command and Control Interoperability Board*), permitiendo

de esta forma avanzar en las necesidades técnico-operacionales de las partes.

Gracias a las gestiones y coordinaciones del CCIB a los largo de varios años de trabajo, el 7 de noviembre de 2017, Chile se transformó en el primer y único país de Latinoamérica y el Caribe en establecer una oficina que le permite gestionar los sistemas COMSEC, la cual se encuentra en dependencias del EMCO en la ciudad de Santiago. Esta oficina agilizará los procesos de distribución de equipamiento y KEYMAT COMSEC a cada una de las fuerzas armadas de Chile, siendo para el caso de la Armada la Dirección de Telecomunicaciones e Informática la encargada de esta materia.

Para la Armada de Chile, los beneficios de obtener permanentemente KEYMAT COMSEC se traducen en la posibilidad de contar con los medios necesarios para otorgar seguridad de comunicaciones a los diferentes sistemas utilizados durante las operaciones navales nacionales, actividades conjuntas y participar activamente en ejercicios internacionales tales como RIMPAC, UNITAS, PANAMAX, entrenamientos DESI y apoyos de control del tráfico marítimo de JIATF-S (sigla de su denominación en inglés *Joint Inter-Agency Task Force - South*).

Los nuevos y futuros desarrollos.

Los sistemas COMSEC no se encuentran exentos a los avances tecnológicos existentes a nivel mundial, los cuales también tendrán una importante relación con las fuerzas armadas de Chile a través del CCIB.

La migración del sistema LINK-11 a LINK-22 a través del programa multinacional NILE (sigla de su denominación en inglés *NATO Improved Link Eleven*), la migración de IFF Modo 4 a IFF Modo 5 a través del Programa AIMS (sigla de su denominación en inglés *Air Traffic Control Radar Beacon System, Identification Friend or Foe, Mark XII/Mark XIIA, Systems*) y la actualización de los cifradores de voz para comunicaciones tácticas del programa VACM (sigla de su denominación en inglés *VINSON ANDVT -Advanced Narrowband Digital Voice Terminal-Cryptographic Modernization*) serán los nuevos desafíos que las fuerzas armadas deberán enfrentar en los próximos años, permitiéndoles mantener estándares internacionales, pioneros a nivel regional y considerados para los entrenamientos y participación en actividades operacionales a nivel global.

* * *

BIBLIOGRAFÍA

1. http://www.ieee.es/Galerias/fichero/docs_marco/2015/DIEEEM06-2015_Seg_operaciones_Medios_A.AriasGlez.pdf
2. http://www.c4i.org/jp3_13.pdf
3. https://www.nsa.gov/news-features/declassified-documents/cryptologic-histories/assets/files/history_comsec_ii.pdf
4. <https://dialogo-americas.com/es/articles/us-chile-interoperability-soars-new-heights>
5. <http://www.link22.org/>
6. <http://www.militaryaerospace.com/articles/2016/12/cyber-security-cryptographic-secure-voice-communications.html>
7. https://www.anmb.ro/buletinstiintific/buletine/2016_Issue2/MES/317-322.pdf