EL COMANDO DE CIBERDEFENSA ALEMÁN
UN CLARO EJEMPLO DE INTEGRACIÓN

Por MY **PABLO ALEJANDRO CAÑETE**

ARTÍCULO CON REFERATO

En el marco de la reestructuración de las Fuerzas Armadas alemanas, el 5 de abril de 2017 la ministra de Defensa, Ursula von der Leyen creó el Comando del Espacio de Información y Ciber (Kdo CIR)[1]. A partir de ese momento, innumerables artículos y redacciones en el mundo no han dejado pasar ese evento para destacar la conformación de este significativo elemento de ciberdefensa en la República Federal Alemana.

Sin embargo, muchas preguntas hay detrás de esta nueva organización. Entre mujeres y varones, el personal supera las 14.000 personas, es decir solo 2.000 efectivos menos que la Armada alemana. ¿Es la cuarta Fuerza Armada en Alemania? ¿Cuál es su misión? ¿Cómo está organizado? ¿Qué capacidades posee? En mayo de 2019, he tenido la oportunidad de realizar una pasantía en el mencionado comando, lo que me permite responder a los interrogantes. La finalidad del

Palabras Clave:
> Comando
> Ciberdefensa
> Ciberseguridad
> Integración
> Inteligencia estratégica

El Comando del Espacio de Información y Ciber alemán no es una fuerza armada, sino que es un comando conjunto que proporciona apoyo de ciberdefensa a sus fuerzas armadas.

presente trabajo es proporcionar información sobre la misión, las funciones, la organización y las capacidades del Kdo CIR.

¿La cuarta fuerza armada alemana?
Las Fuerzas Armadas alemanas (FFAAA) están conformadas por dos grandes organizaciones: civil y militar, que a modo de fácil comprensión se esboza en la figura 1 con sus respectivos efectivos.

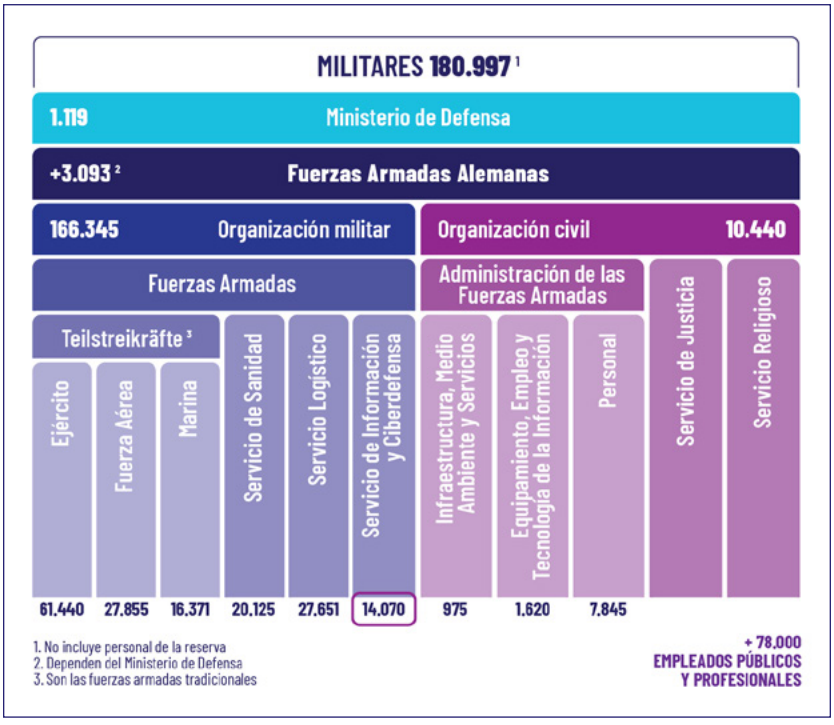
La organización civil normalmente no está relacionada con la parte operacional de las Fuerzas Armadas y en su estructura forman parte las siguientes organizaciones: Infraestructura, Medio Ambiente y Servicios, Equipamiento, Empleo y Tecnología de la Información, Servicio de Personal, Servicio de Justicia y el Servicio Religioso.

La organización militar está estructurada en 6 grandes fuerzas. Las *Teilstreitkräfte* son las Fuerzas Armadas tradicionales, tales como Ejército, Marina y Fuerza Aérea. Poseen además otras 3 organizaciones que los militares alemanes denominan *Organisationsbereiche*. Estas son organizaciones conjuntas, organizadas, equipadas e instruidas para proporcionar apoyo a las FFAAA y comprenden los Servicios de Sanidad, de Logística y el Kdo CIR. Cada fuerza tiene un comandante y depende directamente del Comandante Conjunto de las FFAAA.

Haciendo referencia al primer interrogante, el Kdo CIR no es una Fuerza Armada, sino que es un comando conjunto que proporciona apoyo de ciberdefensa a sus Fuerzas Armadas.

¿El Kdo CIR proporciona sólo apoyo de Ciberdefensa?
La respuesta se obtiene al analizar la misión del Kdo CIR y sus funciones. El Kdo CIR (2019) sostiene que: "así como el Ejército, la Fuerza Aérea y la Marina son responsables de las dimensiones de la tierra, el aire y el mar, también son responsables de manera integral de la dimensión del espacio cibernético y

FIGURA 1. ESTRUCTURA DE LAS FUERZAS ARMADAS ALEMANAS
En el resaltado se visualiza el efectivo del Kdo CIR



Fuente: Bundesministerium der Verteidigung. Recuperado de https://www.bmvg.de (03/05/2019).

1. Kdo CIR: Kommando Cyber- und Informationsraum (Comando del Espacio de Información y Ciber).
2. *Bundeswehr (2019). Servicios del Espacio Cibernético y de la Información.* Recuperado de https://cir.bundeswehr.de/portal

de información [...]"[2]. Además, establece que el mencionado comando garantizará el funcionamiento y la protección del sistema de información de las FFAAA, tanto a nivel nacional como en sus contingentes desplegados en el exterior.

Haciendo referencia a sus funciones, dentro del espacio cibernético y de la información, el Kdo CIR es la máxima autoridad conjunta de comando y control, proporciona además un centro de situación conjunta de información y ciberdefensa a sus Fuerzas Armadas y garantiza la cooperación de organismos nacionales e internacionales en temas relacionados con la quinta dimensión.

Uno de los aspectos más relevantes del mencionado comando es que conduce 3 elementos, como puede verse en la Figura 2. El primer elemento es el Comando de Inteligencia Estratégica, que proporciona apoyo de inteligencia, guerra electrónica, operaciones psicológicas y ciberoperaciones activas. El segundo elemento es el Comando Técnico de la Información que proporciona apoyo de comunicaciones, informática y ciberoperaciones pasivas. El tercer elemento es el Centro de Geoinformación, que proporciona apoyo de información a las ciencias y disciplinas de biología, etnología, teledetección, geodesia, geoinformática, geología, geofísica, geopolítica, hidroacústica, hidrografía, hidrología, cartografía, climatología, meteorología, ecología, oceanografía y fotogrametría.

Entonces, la respuesta a la pregunta inicial es un rotundo no. El Kdo CIR es un elemento conjunto, que integra capacidades de comunicaciones, informática, guerra electrónica, inteligencia, ciberdefensa, operaciones psicológicas e información de diferentes ciencias y disciplinas para proporcionar apoyo a sus Fuerzas Armadas, dentro y fuera del país.

En síntesis, el Kdo CIR funciona como un sistema conjunto que a través de la interoperabilidad de sus medios (personal y material) proporciona capacidades de C4I2SR[3] a sus Fuerzas Armadas desplegadas dentro o fuera de Alemania, tales como misiones de la Organización del Tratado Atlántico Norte (OTAN), de la Unión Europea (UE) y de la Organización de las Naciones Unidas (ONU).

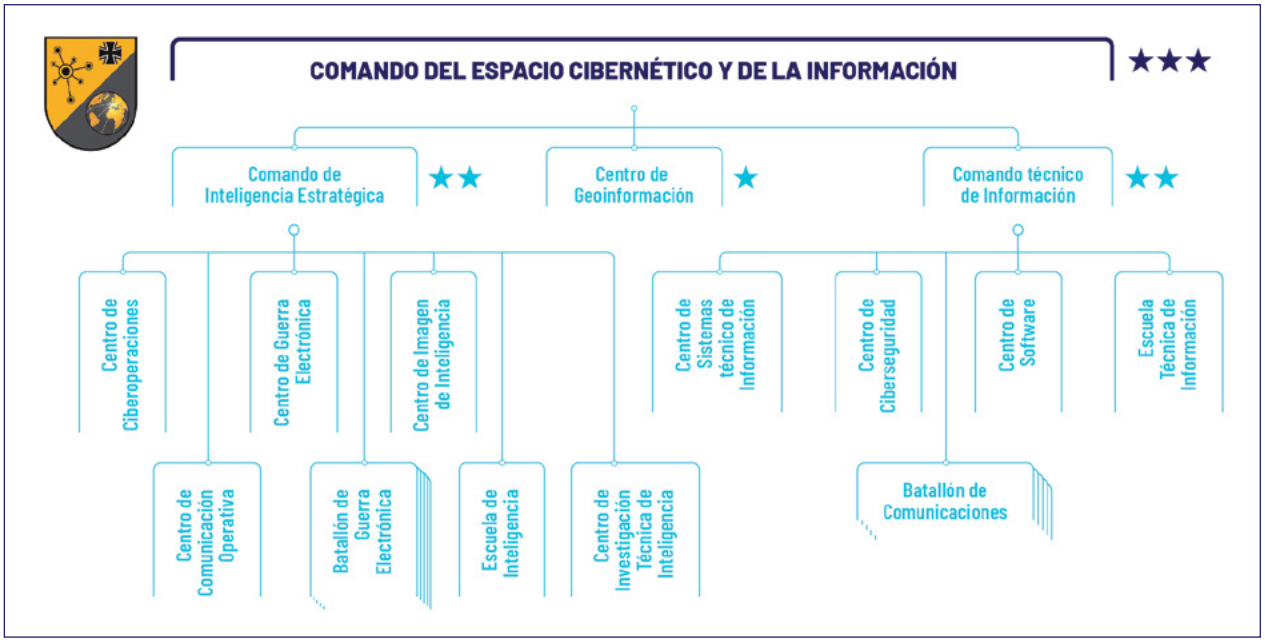
Organización del Kdo CIR

El Kdo CIR tiene a cargo 3 elementos. Su comandante es un general de 3 estrellas. A continuación, se describen la misión de cada uno de ellos y una breve descripción de sus capacidades.

Comando de Inteligencia Estratégica

Tiene la misión de proporcionar apoyo de inteligencia, guerra electrónica, operaciones psicológicas y ciberdefensa a sus Fuerzas Armadas. De izquierda a derecha en la Figura 2, se visualizan sus organizaciones dependientes. El Centro de Ciberoperaciones tiene la capacidad de ejecutar ciberoperaciones activas y el Centro de Comunicación Operativa proporciona apoyo de operaciones psicológicas. Este último Centro conduce la radio y televisión de las FFAAA para personal en el exterior. La radio se llama *Andernach*[4]. Además planifica y conduce medios masivos de comunicación

FIGURA 2 . ORGANIZACIÓN DEL COMANDO DEL ESPACIO DE INFORMACIÓN Y CIBERDEFENSA



Fuente: Das Führungsunterstützungskommando der Bundeswehr 2013-2017 (p.290)

Uno de los aspectos más relevantes del comando es que conduce 3 elementos, el primero es el Comando de Inteligencia Estratégica, el segundo es el Comando Técnico de la Información y finalmente el tercer elemento es el Centro de Geoinformación.

compuesto por personal autóctono de Afganistán, como es la multimedia Bayan Shamal Mediencenter in Mazar-e Sharif[5].

El tercer elemento del Comando de Inteligencia Estratégica es el Centro de Evaluación de Guerra Electrónica. Esta organización es responsable de analizar, identificar, evaluar y registrar toda información relacionada con el espectro electromagnético. Además, tiene como tarea el control técnico sobre los 4 batallones de guerra electrónica. Con respecto a los mencionados batallones, su misión es proporcionar apoyo de guerra electrónica. Sin embargo, cada uno difiere conforme a su misión. Algunos tienen capacidades ofensivas y defensivas de guerra electrónica, tanto en el espectro electromagnético terrestre, naval o aéreo. Otros batallones poseen estaciones fijas de guerra electrónica y todos tienen elementos móviles de guerra electrónica.

Otro elemento perteneciente al Comando de Inteligencia Estratégica es el Centro de Imagen de Inteligencia. Esta organización debería formar parte del Centro de Información de las FFAAA, pero la diferencia radica en que no solo produce información de imágenes satelitales sino que es un centro de interpretación de imágenes. Emplea medios como el radar de reconocimiento SAR-Lupe[6] de las FFAAA, el sistema francés Helios II y productos satelitales del Centro Europeo de Satélites.

La siguiente organización es la Escuela de Inteligencia Estratégica de las Fuerzas Armadas, cuya misión es la formación y perfeccionamiento de los soldados alemanes en el área inteligencia. El último elemento es el Centro de Investigación de Inteligencia Técnica cuya competencia es desarrollar nuevas capacidades técnicas en el espectro electromagnético.

Centro de Geoinformación

Este organismo tiene más de 50 años de experiencia. Su misión es obtener, preparar, actualizar y proporcionar no solamente informes meteorológicos o cartas topográficas a las Fuerzas Armadas, sino también información en los campos de biología, etnología, teledetección, geodesia, geoinformática, geología, geofísica, geopolítica, hidroacústica, hidrografía, hidrología, cartografía, climatología, meteorología, ecolo-

3. Command, Control, Communications, Computers, Intelligence, Information, Surveillance, and Reconnaissance (comando, control, comunicaciones, computación, inteligencia, información, vigilancia y reconocimiento).
4. https://www.radio-andernach.bundeswehr.de/
5. https://www.facebook.com/Bundeswehr/posts/731725646892030
6. https://cir.bundeswehr.de/portal/a/cir/start/dienststellen/ksa/zabbaufkl
7. https://cir.bundeswehr.de/portal/a/cir/start/dienststellen/zgeobw

cv

PABLO ALEJANDRO CAÑETE

El Mayor Pablo Alejandro Cañete egresó como Subteniente del Arma de Comunicaciones en el año 1999 y pertenece a la promoción 130 del CMN. Es Oficial de Estado Mayor y Licenciado en Matemática Aplicada. Posee la Aptitud Especial de Capacitación Antártica. Realizó el Curso de Capacitación del Espectro Electromagnético en Francia (Paris). Actualmente está cursando la Escuela de Guerra en la República Federal de Alemania (Hamburgo).

En Alemania hay una verdadera concientización en lo que respecta a ciberseguridad, confían en la seguridad de su red y si hay que esperar porque el sistema operativo lo demanda, utilizan un refrán breve y contundente: "hasta los comandantes esperan".

gía, oceanografía y fotogrametría[7]. Este Centro trabaja conjuntamente con el Servicio Meteorológico Alemán y su comandante es un general de 1 estrella.

Comando Técnico de Información

Su misión es proporcionar apoyo de comunicaciones, informática y ciberoperaciones defensivas a las FFAAA. Su comandante es un general de 2 estrellas y posee 5 organizaciones.

En la Figura 2, de izquierda a derecha, se visualiza en primer lugar al Centro de Sistemas Técnico de Información. Este administra todas las facilidades de comunicaciones e informática de las FFAAA. Es el nexo directo entre los proveedores de tecnología de información y comunicación (TIC) privados y las Fuerzas armadas. Además, gestiona la asignación de frecuencias y anchos de banda para los enlaces satelitales requeridos en cada operación, asigna frecuencias en las bandas militares a todos los elementos de las FFAAA. Con respecto a los proveedores privados TIC, estos conforman una sociedad privada llamada BWi[8]. Esta empresa es la proveedora directa de servicios TIC para las FFAAA y está compuesta por empresas relevantes tales como Siemens, IBM y Telecom, entre otras. El mencionado Centro de Sistemas administra también los telepuertos satelitales y monitoriza los satélites militares Satcom Bw-1 y Satcom Bw-2 que poseen las FFAAA.

El segundo elemento que forma parte de este comando es el Centro de Ciberseguridad de las Fuerzas Armadas. Su misión es ejecutar operaciones de ciberdefensa pasivas. El Centro de Ciberseguridad posee 2 departamentos y 3 grupos, como puede verse en la Figura 3. El departamento de operaciones planifica y conduce las operaciones de ciberdefensa pasivas de las FFAAA. El departamento *Cyber Security Operations Center* (CSOC) ejecuta la vigilancia, observación, analiza los riesgos de las ciberamenazas y conduce el *Computer Security Incident Response Team* (CSIRT) de las FFAAA.

El Grupo Protección y Prevención realizan actividades y tareas para fomentar la concientización de la seguridad a los usuarios de las redes informáticas de las FFAAA, y es el responsable de estandarizar las técnicas de ciberdefensa y protege los sistemas de armas de las Fuerzas Armadas.

En este punto es necesario destacar algunos aspectos cuya relevancia contribuye a la ciberseguridad de una gran organización como son las Fuerzas Armadas.

En primer lugar, el sistema operativo que emplean las FFAAA es Windows de Microsoft. La herramienta que usan es *Office*. Todos los software son originales y han adquirido la licencia para su uso. Además, está prohibido el empleo

FIGURA 3 . ORGANIZACIÓN DEL CENTRO DE CIBERSEGURIDAD DE LAS FUERZAS ARMADAS ALEMANAS

en los puestos de trabajo de computadoras personales. Las mismas son provistas por las Fuerzas Armadas y solo pueden ser instalado *software* y aplicaciones autorizados. Está terminantemente prohibido el uso de memoria externa tipo USB (*pendrive*) o el empleo de discos duros externos. En los puestos de trabajo, la conexión a intranet o Internet es a través de conexión alámbrica, o sea por cable UTP/STP *(Unshielded Twisted Pair)/(Shielded Twisted Pair)*[9]. Además, en lugares como sala de reuniones, aulas u oficinas con clasificación de seguridad relevante, existen inhibidores de señal de telefonía celular.

En efecto, hay una verdadera concientización en lo que respecta a ciberseguridad. Se imparten innumerables instrucciones y presentaciones en unidades militares y particularmente en la Escuela de Guerra alemana. No se pueden detectar civiles, soldados, suboficiales, oficiales ni siquiera comandantes de más de 1 estrella que vulneren por ejemplo la seguridad a través del uso de un *pendrive*. Todos sus trabajos o presentaciones están en intranet. Confían en la seguridad de su red y si hay que esperar porque el sistema operativo necesita reiniciarse o porque la red está un poco lenta para bajar una presentación de *power point* por ejemplo, el *slogan* es breve y contundente: "hasta los comandantes esperan". Ordenadores provistos, licencia de *software* adquirida, conectividad alámbrica, prohibición de *pendrive* o discos duros externos, inhibidores de señal de telefonía celular en áreas sensibles de información y, por sobre todas las cosas, concientización sobre la seguridad informática. Esas son las bases de la ciberseguridad.

El Grupo Seguridad y Acreditación forman parte también del Centro de Ciberseguridad. Esta pequeña organización es responsable de acreditar y asesorar en lo concerniente a seguridad informática y proyectos TICs. Es el organismo nexo entre las FFAAA y las industrias TICs en materia de seguridad informática. Por último, el Grupo Control y Apoyo ejecuta pruebas de penetración y da seguridad en las redes.

El Comando Técnico de Información conduce 7 batallones de Comunicaciones, de los cuales 6 son conjuntos y 1 combinado en apoyo a las fuerzas de la OTAN. Los mencionados elementos proporcionan apoyo de comunicaciones e informática a los elementos desplegados fuera del territorio de Alemania, por ejemplo contingentes de la OTAN, la UE u ONU. Eventualmente, podrá proporcionar apoyo a las divisiones del ejército alemán o a otros elementos de otras Fuerzas Armadas. Es necesario resaltar que las 3 divisiones del ejército alemán tienen su elemento de comunicaciones dentro de sus formaciones y además, cada brigada posee en su orgánica una compañía de comunicaciones. Otro aspecto relevante es que los mencionados batallones son conducidos por el segundo comandante del Comando Técnico de Información y no por su comandante.

En nuestra estadía, hemos visitado el batallón de Comunicaciones 282 ubicado en Kastellaun (Renania del Norte) y el batallón de Comunicaciones 293 situado en Murnau (Baviera). Los batallones normalmente están organizados por 5 compañías. Difieren mínimamente en su estructura, pero en general cuentan con una compañía de redes locales, de comunicaciones satelitales, radioeléctrica, de comunicaciones troncalizadora (facilidad radioeléctrica de *trunking*) y una compañía comando y servicios que no posee elementos de sanidad porque lo proporciona el Servicio de Sanidad de las FFAAA, tal como se explica en la Figura 1. En general las mencionadas compañías tienen similares misiones, funciones, actividades y tareas de acuerdo a lo especificado en la doctrina de la OTAN.

Con respecto a la cultura de la organización, es importante resaltar que los batallones están compuestos por personal de las 3 Fuerzas Armadas. Por ejemplo, el jefe de batallón puede ser del Ejército y su segundo jefe o el oficial de operaciones (S-3) de la Fuerza Aérea o de la Armada. La integración del personal culturalmente está totalmente asimilada.

El Centro *Software* de las FFAAA es otra organización del comando técnico de información. Este elemento desarrolla, prueba, controla e integra *software* de gestión, operación y simulación de las Fuerzas Armadas. Trabaja en conjunto con el organismo federal de equipamiento, tecnología e información y empleo para las FFAAA, en proyectos como HaFis (*Harmonisierung der Führungsinformationssysteme*). Es un proyecto para integrar el sistema C4I2SR de las FFAAA que sea a la vez interoperable con el sistema de la OTAN y con algunos sistemas para misiones de la UE y de la ONU. El centro Software trabaja con la licencia del *Virtual Battle Space,* que es una simulación con armamentos y procedimientos de la FFAAA, ambientado en escenarios reales tales como Afganistán (misión de la OTAN) o MALI (misión de la ONU). El Centro certifica además todos los *Software* que emplean las FFAAA.

La última organización del comando es la Escuela Técnica de Información. Es el centro de capacitación del personal de las Fuerzas Armadas relacionado con comunicaciones, informática, ciberdefensa y guerra electrónica. Actualmente, está emplazada en Feldafing, pero el siguiente año será trasladado a sus nuevas y modernas instalaciones en Pöcking. Ambas ciudades se sitúan en Baviera.

El Kdo CIR, a través de escuela de formación y perfeccionamiento, ha

8. https://www.bwi.de
9. Par trenzado apantallado/Par trenzado blindado.

Es necesario resaltar que las tres divisiones del ejército alemán tienen su elemento de comunicaciones dentro de sus formaciones y además, cada brigada posee en su orgánica una compañía de comunicaciones.

realizado acuerdos con firmas privadas de TICs para que el personal de suboficiales y soldados realice un curso de especialización en TICs en solo 21 meses. Al término del curso, los suboficiales son certificados para trabajar en cualquier empresa de TICs cuando finalicen su carrera militar. Es importante resaltar este aspecto porque la capacitación técnica en Alemania dura normalmente 3 años. Es una buena motivación para el ingreso de personal a las FFAAA. La escuela recibe anualmente un promedio de 7.000 cursantes de las FFAAA y dictan, aproximadamente 170 cursos.

Conclusiones finales

El Kdo CIR no es una Fuerza Armada, sino un comando conjunto que posee innumerables capacidades, una de ellas es la ciberdefensa. El comando cuenta actualmente con un efectivo de más de 14.000 militares y civiles y prevé arribar al año 2022 con alrededor de 15.000, o sea aproximadamente la misma cantidad de efectivos que la Armada alemana.

El Kdo CIR planifica, organiza y conduce los apoyos de comunicaciones, informática, guerra electrónica, inteligencia, ciberdefensa (operaciones defensivas y ofensivas), operaciones psicológicas y geoinformación de las Fuerzas Armadas alemanas para proporcionar capacidades de C4I2SR a las misiones en el exterior (OTAN, EU u ONU) o ante la necesidad particular de alguna Fuerza Armada en la República Federal de Alemania.

En lo concerniente a educación, este comando es responsable de la capacitación no solo del área de ciberdefensa sino también de comunicaciones, informática, inteligencia y guerra electrónica de las FFAAA. Con respecto a la cultura de la organización, la integración del personal de las tres Fuerzas Armadas lo tiene totalmente asimilado.

El Kdo CIR es un claro ejemplo del principio de la conducción denominado integración, permite lograr la mayor interoperabilidad de sus medios (personal y material) a través de la integración de las capacidades de comunicaciones, informática, inteligencia, guerra electrónica, ciberdefensa, operaciones psicológicas y geoinformación en sus Fuerzas Armadas. Mientras que en algunas Fuerzas Armadas de otros países continúan aun debatiendo si las operaciones de ciberdefensa son de la competencia de comunicaciones, de informática o inteligencia, sin embargo, el Kdo CIR las ha integrado.

En las guerras actuales, las Fuerzas militares se caracterizan por contar con elementos pequeños, rápidos, autosostenibles e interoperables con un moderno sistema C4I2SR. El Kdo CIR ha cumplido con uno de esos requisitos y es por ello un claro ejemplo de integración. ▮

AGRADECIMIENTOS

General de División (R)
Evergisto de Vergara
–
Brigadier Mayor
Alejandro Moresi
–
Teniente Coronel
Jürgen Nehring
–
Teniente Coronel
Jan Wilheine
–
Mayor (R)
Alejandro Corletti
–
Mayor
Oscar Gómez