# SECCIÓN No. 1:
## Enfocada en la tecnología : Escenario nacional de la aplicación de las innovaciones tecnológicas

Seguridad, Ciencia & Defensa, Año IV, Nº 4, 2018, pp. 11-20

# Innovaciones tecnológicas en las Fuerzas Armadas de República Dominicana ante nuevos escenarios de conflictos

## TECHNOLOGICAL NEEDS IN THE ARMED FORCES OF DOMINICAN REPUBLIC BEFORE NEW SCENES OF CONFLICTS

***Recibido: 13 / 06 / 2018*** ***Aprobado: 21 / 09 / 2018***

Capitán de Corbeta
**Fausto R. Richardson Hernández**
Armada República Dominicana

En la actualidad el autor está en la fase de culminación de tesis de un Doctorado en Proyectos con la Universidad Internacional Iberoamericana (UNINI – México). El tema de tesis es "Modelo para potenciar la integración de las TIC en la educación primaria en República Dominicana. Caso de estudio: Escuelas públicas del Municipio de Santo Domingo Oeste". Obtuvo su formación inicial con una Licenciatura en Informática en la Universidad Pedro Henríquez Ureña (UNPHU), en el año 2003. Ha fortalecido sus conocimientos a través de la titulación de Máster en Gestión Universitaria con la Universidad de Alcalá, España, en el año 2015; y una Maestría en Sistemas de Información con el Stevens Institute of Technology, USA, para el año 2011. También cuenta con diversas especialidades, entre ellas: Especialidad en Derechos Humanos y Derecho Internacional Humanitario (2011) y una especialización en Seguridad Nacional relacionada a la Ciberseguridad (2018). En su formación técnica profesional domina el uso de los lenguajes de programación y las bases de datos; las redes y su seguridad; los temas relacionados a la Ciberseguridad; y las buenas prácticas existentes en el ámbito de las Tecnologías de la Información y Comunicación. faustorichardson@gmail.com

# RESUMEN

Desde la segunda mitad del siglo pasado (S. XX), fue marcado el inicio de la computación luego de finalizada la Segunda Guerra Mundial, en donde quedó claramente evidenciado que la supremacía de una nación iba a depender en algún momento de su poder económico y militar de la mano con su capacidad de innovación tecnológica. Esto quedó confirmado con el surgimiento del fenómeno industrial mundial, más bien conocido como: globalización. La industria, que favorece el desarrollo económico y financiero de una nación, obliga al desarrollo de tecnologías que permitan agilizar el análisis e intercambio de información para la toma de decisiones, asunto el cual favorece de manera colateral el poder militar. En ese sentido, las nuevas Tecnologías de la Información y Comunicación(TIC) han producido un nuevo escenario de conflicto armado acompañado de amenazas a la seguridad y defensa nacional, en donde el combate es integrado de manera virtual (con inteligencia artificial, comunicaciones, aplicaciones informáticas, robótica, entre otros aspectos), lo que se conoce como ciberespacio. El presente artículo busca despertar el interés en cuanto a la importancia de las innovaciones tecnológicas militares, de manera directa, la importancia de contar con un C4i (Comando / Control / Comunicaciones / Computación / Inteligencia) como centro de operaciones para el intercambio de información de las operaciones militares en las Fuerzas Armadas de la República Dominicana, y la conformación de un CSIRT para salvaguardar la confidencialidad, integridad y disponibilidad de esta infraestructura en el intercambio de las informaciones que allí se generan.

**Palabras clave:**

C4i, innovaciones tecnológicas militares, CSIRT, CERT, información, TIC.

## ABSTRACT

From the second half of the last century (S. XX), was marked the beginning of computing after the end of the Second World War, where it was clearly demonstrated that the supremacy of a nation was going to depend at some point on its economic power and military hand in hand with its capacity for technological innovation. This was confirmed with the emergence of the global industrial phenomenon known as: globalization. The industry, which favors the economic and financial development of a nation, requires the development of technologies that make it possible to speed up the analysis and exchange of information for decision making, a matter that favors collateral military power. In this sense, the new Information and Communication Technologies (ICT) have produced a new scenario of armed conflict accompanied by threats to national security and defense, where combat is integrated virtually (with artificial intelligence, communications, applications, computer science, robotics, among other aspects), what is known as cyberspace. This article seeks to awaken interest in the importance of military technological innovations, directly, the importance of having a C4i (Command / Control / Communications / Computing / Intelligence) as a center of operations for the exchange of information of the military operations in the Dominican Republic Armed Forces and the conformation of a CSIRT to safeguard the confidentiality, integrity and availability of this infrastructure in the exchange of the information generated there.



**Keywords:**

C4i, technology innovations, CSIRT, CERT, information, ICT.

## Introducción

Luego de finalizada la Segunda Guerra Mundial, se han realizado innumerables análisis de los diferentes elementos que incidieron a favor de los países aliados[1] para que estos se repusieran de lo que sería una clara derrota ante el gran imperio que en la época representaba la famosa Alemania Nazi.

En los análisis se ha hecho énfasis a las estrategias utilizadas en las diferentes batallas libradas, en especial, a la más épica hazaña para garantizar la victoria representada en lo que fue la "Operación Overlord[2] ", más bien conocida como la Batalla de Normandía, iniciada con el famoso desembarco llevado a cabo el 6 de junio de 1944 en Normandía, precisamente en las playas de la citada ciudad.

Sin embargo, esta batalla (y otras más que fueron libradas) posiblemente no se hubiese podido llevar a cabo, de no ser por los aportes que hicieron durante la guerra un grupo de notables científicos liderados por el famoso Alan Turing, quienes construyeron un mecanismo electrónico que fue capaz de poder descifrar los códigos de comunicación encriptados a través de la famosa máquina enigma, creada por los alemanes para cifrar sus mensajes y poder así ocultar la información que intercambiaban a través de estos. Este elemento científico (y por qué no también tecnológico), no solo ayudó en gran manera al triunfo obtenido por los aliados, sino que también, a recortar en tiempo y pérdidas la Segunda Guerra Mundial.

Es a partir de este escenario bélico que inicia la carrera entre las grandes potencias por el desarrollo de la ciencia de la computación, en especial, el período de la llamada "Guerra Fría", buscando adelantos científicos y tecnológicos en la creación de mecanismos y dispositivos que les permitiera procesar y transmitir datos para así convertirlos en información valiosa, tomando gran notoriedad todos los aportes científicos que ya venía presentando Turing, principalmente con su famosa

1 Las principales potencias que conformaron el bando de países aliados fueron: Gran Bretaña, Francia (exceptuando el período de su ocupación por Alemania 1940-1944), la URSS (desde la agresión alemana en junio de 1941), Estados Unidos (desde la agresión japonesa en diciembre de 1941) y China, que ya peleaba contra Japón desde 1937, antes del estallido de la guerra general.

2 Jefes supremos.

"Máquina de Turing", dispositivo hipotético que representaba lo que es hoy día una máquina de computación (es decir el computador).

Finalizada ya la guerra fría a principio de los años 90, y en ese mismo período de tiempo el inicio del auge del internet a través del nacimiento de la web, nace un fenómeno económico, que apoyado en la tecnología (entre otros factores), hace apertura de los grandes mercados del mundo, al mismo tiempo que impulsa el desarrollo permanente y acelerado de nuevas herramientas tecnológicas y la adopción de manera casi obligatoria de estas por las naciones a nivel mundial como una manera de mantener su competitividad en esta nueva modalidad de comercio que hoy día conocemos como: Globalización.

Estos dos escenarios, uno de índole militar y el otro un nuevo modelo industrial, tienen como común denominador la gestión de la información a través de las herramientas tecnológicas que han sido creadas para lograr esta tarea de la manera más eficiente posible. Las herramientas tecnológicas a las que se hacen referencia, es lo que se conoce hoy día como Tecnologías de la Información y la Comunicación (TIC).

Es de esta manera como nace un nuevo escenario de conflicto que ha de llevar a realizar grandes cambios estratégicos en el arte de la guerra y los conflictos armados, el ciberespacio, en el cual se hace necesario para preservar la seguridad nacional el garantizar la confidencialidad, la integridad y disponibilidad del elemento fundamental para la toma de decisiones: la información.

En resumen, a partir de los cambios fundamentales que son generados por las sociedades y el mundo a través de la industria, las operaciones militares capitalizarán cada vez más los avances y ventajas que ofrecen las TIC para garantizar la defensa y seguridad de la nación.

# Desarrollo del tema

## 1) La evolución de la tecnología militar

El avance tecnológico que podemos apreciar hoy día, no solo ha incidido en mejorar el nivel y la forma en cómo la sociedad del presente siglo se desarrolla desde el ámbito educacional hasta el de mejorar continuamente las técnicas y métodos del comercio y la industria para mantener sus niveles de competitividad productiva.

De manera colateral, el sector militar ha ido evolucionando en cuanto a sus capacidades técnicas en lo que respecta a su armamento, con el fin de poder dar respuesta a los nuevos escenarios de conflictos armados a los cuales nos hemos referido, y de igual manera, a los demás entornos de combate (tierra, mar y aire) que el avance tecnológico ha fortalecido con grandes mejoras al armamento convencional utilizado.

De acuerdo a Salazar (2014), en el siglo XXI todos los sistemas de armas y tecnología militar en general han experimentado grandes avances técnicos que han incrementado sus prestaciones y su valor militar en un nuevo modelo de la relación entre la concentración y dispersión militar, y entre la potencia y movilidad de una fuerza armada. En ese mismo sentido añade el autor, que se han producido grandes cambios en la movilidad de unidades militares; el alcance de las fuerzas navales y aéreas; y el alcance y precisión de las armas.

Todo este avance tecnológico en el aspecto militar se debe al desarrollo de aplicaciones informáticas, el avance de los medios de comunicaciones, la electro-óptica, la tecnología láser, los sensores, la robótica y la tecnología espacial, esta última en aspectos tanto en sistemas de propulsión como en plataformas orbitales, que han permitido procesar los datos con mayor exactitud, y convertirlos así, en informaciones más precisas que garanticen el éxito de las operaciones militares con la toma de decisiones oportunas del alto mando.

Gráfica No. 1 – Soldado calibrando su casco con mira nocturna, gracias a la electro-óptica.

Gráfica No. 2 – Soldado utilizando un lanza cohetes con tecnología láser

Toda esta revolución tecnológica militar ha conllevado a la creación de nuevos modelos de teatros operacionales, en donde se integran funciones y medios militares mediante la aplicación sistemática de tecnologías, cuyo proceso ha sido descrito por Lawrence Freedman, como una revolución en asuntos estratégicos que ha transformado el escenario a partir del fin de la Guerra Fría. (Salazar, 2014).

Ya se sabe, que hoy día (más que nunca), el manejo eficiente de la información es lo que impulsa la eficacia del éxito

de las estrategias que son trazadas en las operaciones militares, lo que permite cumplir con mayor éxito la misión de unas Fuerzas Armadas. Esto se debe a que el Alto Mando Militar debe de contar con el respaldo de herramientas que les permitan acelerar el proceso de planificación y toma de decisiones para lograr la superioridad.

Por lo que a lo que se refiere Freedman, es a la integración del Mando, Control, Comunicaciones, Computadoras e Inteligencia (C4i). Este nuevo método de trazar las estrategias en los nuevos escenarios de conflictos armados, hace denotar la superioridad técnica de toda fuerza armada que lo ha implementado, debido a que impulsa el proceso de utilizar las mejores herramientas tecnológicas que permitan llevar a cabo operaciones efectivas en la defensa y seguridad de la nación.

## 2) EL C4I


Gráfica No. 3 - Modelo conceptual de un C4i

### 2.1 Definición

Un Centro de Comando-Control-Comunicación-Computación-Inteligencia (C4I), es el centro de mando operacional, que como he señalado anteriormente, es la representación idónea para el manejo de la información entre fuerzas, utilizando la integración de herramientas tecnológicas como apoyo a las estrategias operacionales, lo que permitirá incrementar significativamente la probabilidad de éxito de las operaciones militares, potenciando la listeza operacional de una Fuerza Armada.

Así mismo lo expresan Kramer, Wentz y Starr (2009), cuando señalan que en los últimos 30 años, ha causado una gran revolución e impacto en la conducción de las operaciones militares el manejo de la información. En ese mismo sentido añaden, que en los Estados Unidos se ha producido un fenómeno llamado "Guerra Centrada en la Red"[1] , donde se combinan las comunicaciones compartidas, la data que es clave recopilar para posteriores análisis, la capacidad de análisis del personal para convertir esa data en información que permita al Alto Mando Militar realizar tomas de decisiones en las operaciones (antes, durante y después), y lograr un alto nivel de efectividad y agilidad operacional.

Es decir, que el uso apropiado que se hace de la tecnología en todas las fuerzas que componen una Fuerza Armada, a través de un C4i, se podrán unificar todas estas herramientas para lograr una gestión de la información con

1 La guerra centrada en redes es una doctrina militar que apunta a convertir una ventaja informativa (facilitada en parte por las tecnologías de información y comunicación) en una ventaja competitiva mediante una sólida red de fuerzas, geográficamente dispersas, pero bien conectadas e informadas.

mayor fluidez que lo habitual, logrando la efectividad operacional señalada en los diferentes escenarios de conflictos armados.

Esto permite que una de las capacidades más importantes que los sistemas C4i brindan a los comandantes es la conciencia situacional, es decir, la información sobre la ubicación y el estado de las fuerzas amigas y enemigas. En ese sentido, el C4i se convierte en un componente necesario para lograr la superioridad en la toma de decisiones, aunque no garantiza por sí solo la toma de decisiones. Esto quiere decir que los comandantes deben tomar los conocimientos pertinentes de comando y combinarlos con su criterio, incluidos los aspectos difíciles de cuantificar del comportamiento humano (como la fatiga, el nivel de experiencia y el estrés), la incertidumbre de los datos y los estados futuros plausibles resultantes de las acciones de su fuerza y la del enemigo.

**2.2 Criterios de implementación de un C4i**

Pero como toda implementación tecnológica, un centro C4i requiere de una serie de criterios (aparte de los técnicos informáticos) a ser considerados para llevar a cabo dicha implementación de manera satisfactoria, entre los que se citan:

1. La integración explícita del uso de las herramientas que brindan las Tecnologías de la Información y Comunicación (TIC) en las operaciones militares. Es decir, debe ser un elemento mandatorio.

2. Incluir estas herramientas TIC como parte del apoyo fundamental de las estrategias operacionales militares. Es decir, que es necesario incluir el uso de las TIC como parte de la Doctrina Militar como herramienta fundamental para la planificación y ejecución de las operaciones militares llevadas a cabo por una Fuerza Armada en el cumplimiento de su misión.

3. Se debe establecer quiénes serían los componentes claves en las operaciones militares como parte esencial de un C4i. Esto quiere decir, que se deben identificar e integrar todos los componentes críticos en las operaciones militares, ya que sería poco posible (y poco efectivo) envolver todos los componentes que componen la estructura organizacional de una Fuerza Armada.

4. Es necesario tener claramente definida la pirámide del mando en este tipo de estructuras operacionales, y en donde cada componente entienda cuál es su rol dentro de la estrategia operacional trazada en los distintos escenarios a afrontar.

5. El uso de las capacidades técnicas como apoyo fundamental para lograr el objetivo de las operaciones. Uno de los objetivos de la puesta en funcionamiento de un C4i es identificar (y maximizar) las capacidades técnicas y tecnológicas de todos sus componentes, y unificarlas para que den apoyo efectivo, armónico, y alineado a las estrategias militares trazadas.

**2.3 Aseguramiento de un C4i**

El C4i es un complejo sistema de sistemas que, como ya hemos visto, permite al comandante militar lograr la superioridad de la decisión al afectar la información del adversario y los procesos basados en la información, pero al mismo tiempo deben ser protegidos sus propios sistemas de información.

Debido a la sensibilidad de la información militar, las amenazas a los C4i son reales. Esto se debe al incremento constante del riesgo en el ciberespacio que eleva las posibilidades de que los sistemas sean vulnerados, por lo que la seguridad de un C4i es un desafío importante para mantener la integridad, la confidencialidad y la disponibilidad de la información dada la compleja arquitectura de estos sistemas.

De acuerdo a Urbaczewski y Mrdalj (2006), han sido establecidos algunos modelos que le brindan la capacidad a las organizaciones de entender y analizar las debilidades e inconsistencias en arquitecturas tecnológicas complejas como los C4i para aplicar los correctivos correspondientes.

El análisis crítico a los diferentes modelos de seguridad diseñados (la mayoría por el Departamento de Defensa de los Estados Unidos, como el DODAF[2] ) necesitaría de un artículo científico expresamente para determinar las características del idóneo a implementarse para asegurar un C4i, pero de lo que está más que seguro el autor de este artículo, es que para garantizar la seguridad del C4i es necesario que en la aplicación de estos modelos exista un Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT[3] ) capaz de dar respuesta a los incidentes con el impacto mínimo aceptado por las organizaciones.

## 3) Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT)

De acuerdo a varios autores (Ruefle,et al., 2014), cuando ocurren incidentes de seguridad informática, es fundamental que las organizaciones puedan manejarlos de manera oportuna. La velocidad con la que una organización puede reconocer, analizar y responder a un incidente afectará el daño y reducirá los costos de recuperación. La gestión organizada de incidentes requiere procesos definidos y repetibles y la capacidad de aprender de los incidentes que amenazan la confidencialidad, disponibilidad e integridad de los sistemas y datos críticos.

En ese sentido, hoy día la responsabilidad de la gestión de estos incidentes recae sobre un Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT). Así mismo opinan también Grobler y Bryk (2010), cuando dicen que un CSIRT es un equipo de especialistas dedicados a la seguridad de la información que se prepara y responde a los incidentes de seguridad de la información.

Sin embargo, también añaden estos autores, que el establecimiento de un CSIRT no está exento de ciertas dificultades o complicaciones. Este tipo de proyectos requiere de un compromiso sostenido y depende en gran medida de un círculo de confianza internacional que necesita tiempo para desarrollarse, y que sin esos atributos, un proyecto de establecimiento de un CSIRT pudiera encontrarse con una serie de problemas con efectos sobre el éxito del proyecto.

## 4) Futuras Investigaciones

Los elementos tomados en consideración en el presente artículo, fundamentan la propuesta de llevar a cabo la puesta en funcionamiento de un C4i y un CSIRT para potenciar la listeza operacional de las Fuerzas Armadas de la República Dominicana. Sin embargo, antes de iniciar este proceso, se requiere realizar en futuras investigaciones un análisis crítico y las recomendaciones pertinentes a los cri-

2 Department of Defense Architecture Framework (DoDAF).

3 Por sus siglas en inglés.

terios que deben de tomarse en consideración para la implementación de un C4i, así como también, a los modelos de seguridad física y electrónica existentes para asegurar este tipo de infraestructuras complejas y la conformación de un CSIRT para dar respuestas a las necesidades de aseguramiento de las mismas.

## Conclusión

Visto lo analizado en el presente artículo, el autor concluye con lo siguiente:

Debido a los avances tecnológicos, hoy más que nunca, el manejo y análisis de datos para ser convertidos en información es un elemento crucial para la toma de decisiones y la planificación estratégica de las operaciones militares.

Las tecnologías que brinda un Centro de Comando – Control – Comunicaciones – Computación – Inteligencia (C4i) se hacen relevantes para hacer efectivas las decisiones de comando que deben ser consideradas y ejecutarse en el proceso de planificación y toma de decisiones en operaciones militares.

Un C4i debe estar asegurado mediante un modelo de seguridad que salvaguarde su estructura física y electrónica, al mismo tiempo de estar equipado por un equipo especializado para dar respuestas a cualquier incidente que atente a su buen funcionamiento, es decir, un CSIRT.

## Referencias Bibliográficas:

Cebrowski, A. K. y Garstka, J. J. (1998, January). Network-centric warfare: Its origin and future. *In US Naval Institute Proceedings*, 124(1), 28-35.

De Salazar Serantes, G. (2014). Cambio tecnológico, conflicto armado y desarme: los rasgos de la transición al siglo XXI. *Cuadernos de estrategia*, (169), 9-38.

Grobler, M. y Bryk, H. (2010). Common challenges faced during the establishment of a CSIRT. In *Information Security for South Africa* (ISSA), 2010 (pp. 1-6).

Kramer, F. D., Starr, S. H. y Wentz, L. K. (Eds.). (2009). *Cyberpower and national security*. Potomac Books.

National Research Council. (1999). *Realizing the Potential of C4I: Fundamental Challenges*. National Academies Press.

Ruefle, R., Dorofee, A., Mundie, D., Householder, A. D., Murray, M. y Perl, S. J. (2014). Computer security incident response team development and evolution. *IEEE Security & Privacy*, 12(5), 16-26.

Urbaczewski, L. y Mrdalj, S. (2006). A comparison of enterprise architecture frameworks. Issues in Information Systems, 7(2), 18-23.