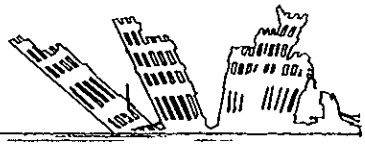
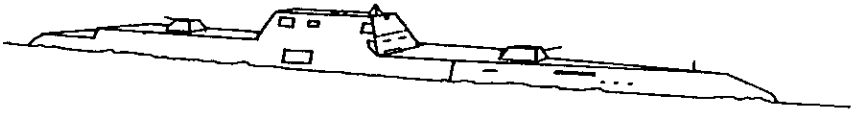
Las Marinas de Guerra después del 11-S





EL IMPACTO DEL 11-S SOBRE LOS SISTEMAS DE MANDO Y CONTROL MILITARES

José Luis DÍEZ DEL CORRAL GARCÍA

Ing. (IAN) (R) (1)

Me enfrenta el director de esta REVISTA con el reto de describir qué influencia han tenido en los Sistemas de Mando y Control Militares (SMCM) los acontecimientos derivados del 11-S.

El tema es amplio y complejo, e intentaré en este artículo crear un marco para encuadrarlo.

Qué es un Sistema de Mando y Control Militar

Definición de Sistema

Sistema es un grupo armónicamente coordinado de elementos de varios tipos:

(1) Durante el periodo de 1 de junio de 1994 a 1 de febrero de 2003 ha sido Científico Principal de la División de Mando, Control y Sensores de la NATO C3 Agency (NC3A).

— Instalaciones.
— Equipos.
— Personal.
— Procedimientos.

Éstos realizan cooperativamente entre ellos y con otros sistemas exteriores unas tareas o funciones que permiten la realización de unos servicios necesarios para cumplir una misión, propósito o fin.

Definición de Mando y Control

Mando y Control son dos términos ampliamente utilizados en el dominio militar:

— *Mando.* Autoridad investida en un individuo. Se puede describir (pero no definir) como el proceso por el cual una Autoridad o Mando imprime su voluntad e intenciones en sus subordinados y comprende la autoridad y responsabilidad para desplegar y asignar fuerzas o recursos para cumplir sus misiones.
— *Control.* Autoridad ejercida por el Mando. Se puede describir (pero no definir) como el proceso por el cual una Autoridad o Mando asistida por su Estado Mayor organiza, dirige y coordina las actividades de las fuerzas asignadas.

Mando y Control representan pues dos caras de la misma moneda, mutuamente dependientes. Es inútil tener autoridad investida si no se puede ejercer, y viceversa.

Estas funciones de Mando y Control suelen venir asociadas o complementadas con la función de Consulta: responsabilidades y actividades de las autoridades políticas, militares y civiles en la consulta política, incluyendo control de crisis, consulta nuclear y planeamiento de procedimientos ante emergencias civiles.

Estas tres funciones básicas juntas forman el dominio C3 (2), *Consultation Command and Control.*

La siguiente figura extraída del AAP-31(A) (3) representa el llamado Modelo Semántico Conceptual del Dominio C3 en NATO.

---

(2) En algunos documentos obsoletos se conservaba la tercera C para *Communications*, en forma errónea, pues mezclaba al mismo nivel objetivos o funciones básicas *(Command and Control)* con medios o instrumentos *(Communications).*

(3) *NATO Glossary of Communication and Information Systems Terms and Definitions.*

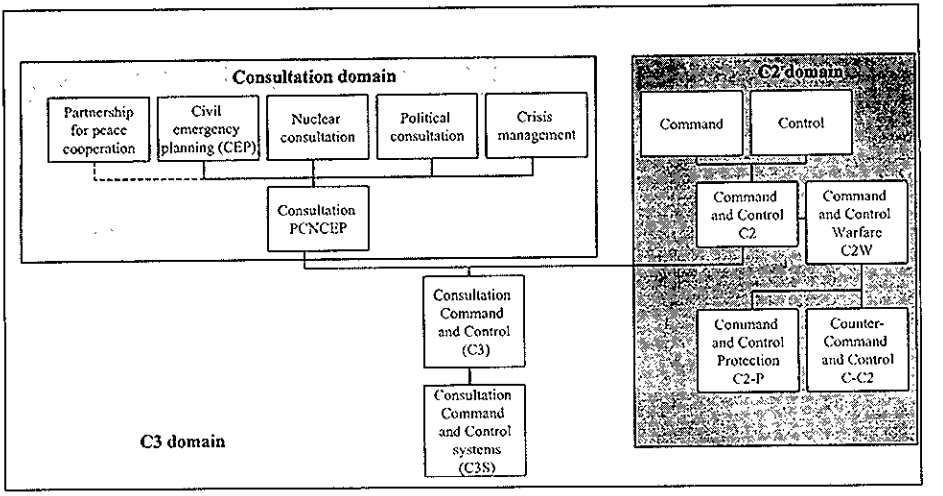


Figura 1. Modelo Semántico Conceptual para el Dominio NATO C3.

Modelo Conceptual de los Sistemas de Mando y Control Militar (SMCM)

El propósito de los Sistemas de Mando y Control Militares es el Mando y Control de las Fuerzas Armadas y sus recursos asociados en el desarrollo de operaciones militares para cumplir los objetivos militares.

El Sistema de Mando y Control Militar está soportado por dos sistemas más genéricos: Sistema de Gestión de la Información *(Management Information System,* MIS) y Sistema de Comunicaciones que deben ser particularizados para el propósito específico de las operaciones militares. Para completar los componentes del SMCM, debemos añadir los Sensores (4) y las Instalaciones o Cuarteles Generales desde donde se ejerce el Mando y Control.

En resumen, un SMCM tiene los siguientes componentes:

— Sistema de Información de Mando y Control.
— Sistema de Comunicaciones de Mando y Control.
— Sensores.
— Instalaciones y Cuarteles Generales de Mando y Control.

Las figuras 2-a y 2-b presentan el Modelo Semántico Conceptual de los Sistemas NATO C3, también extraído del AAP-31 (A).

(4) Dependiendo de la realización específica, el «sensor» puede ser un componente sencillo, una instalación más compleja o un verdadero sistema.

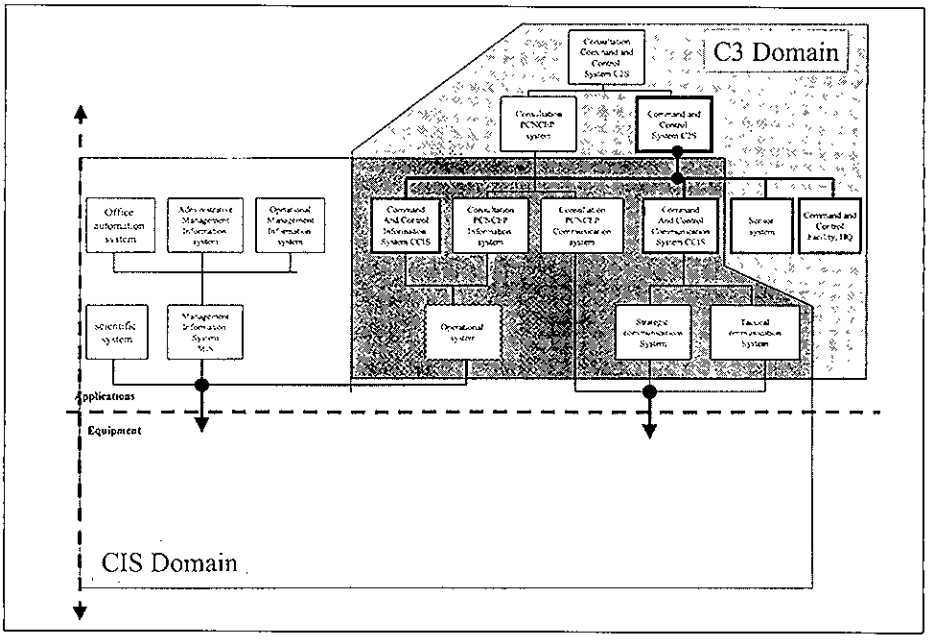


Figura 2-a. Modelo Semántico Conceptual para los Sistemas NATO C3 y Sistemas de Comunicaciones e Información (Aplicaciones).

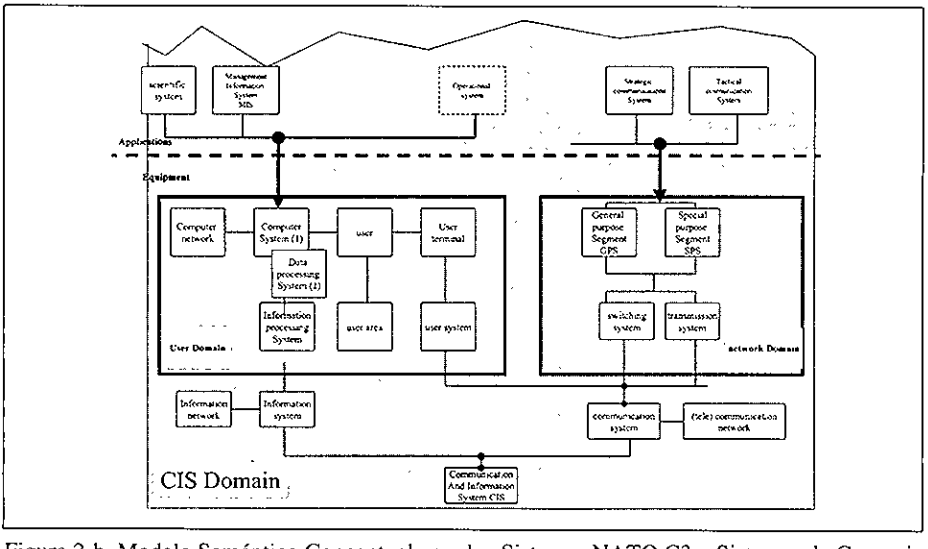


Figura 2-b. Modelo Semántico Conceptual para los Sistemas NATO C3 y Sistemas de Comunicaciones e Información (Equipos).

Arquitectura Operativa de los Sistemas de Mando y Control Militar (SMCM)

Para establecer una Arquitectura Operativa de los SMCM se necesita considerar varios ejes o categorías que determinan su contexto.

a) Niveles Militares.

Los SMCM se articulan en tres niveles desde donde se despliega la estructura de Mando en forma jerarquizada:

— *Nivel Estratégico*, para el Mando y Control de fuerzas utilizadas dentro de un marco político y de forma sincronizada con otras iniciativas no-militares (diplomáticas y económicas, por ejemplo). A este nivel corresponden el análisis de riesgo de la acción militar, los planes estratégicos y la determinación global de fuerzas y recursos necesarios.
— *Nivel Operacional*, donde las operaciones conjuntas (entre distintos servicios) y combinadas (entre naciones) se planifican globalmente, se ejecutan y se apoyan logísticamente dentro del teatro de operaciones para conseguir los objetivos estratégicos.
— *Nivel Táctico*, donde las fuerzas se emplean en acciones militares para conseguir los objetivo militares inmediatos que en conjunto permitirán el cumplimiento de los objetivos operacionales y, estos a su vez, los objetivos Estratégicos.

b) Estructura Jerárquica de Mando.

En íntima relación con los Niveles Militares, se encuentra la Estructura Jerárquica de Mando, que puede ser permanente y geográficamente fija o temporal con capacidad para ser desplegada *(deployable)* en la zona geográfica más conveniente, y la Estructura de Fuerzas sobre las que se ejercita el Mando y Control.

En términos OTAN estamos hablando de la Estructura OTAN de Mando Estática (figura 3) y de la Estructura para fuerzas de tareas Combinadas-Conjuntas —*Combined Joint Task Force* (CJTF) *Structure*— (figura 4).

Todo el proceso ha sido resumido perfectamente por el capitán de navío Buenaventura López Rodríguez y el comandante de Infantería de Marina Andrés Gancio Painceira en un artículo en esta REVISTA al que me remito (5).

(5) Ver REVISTA GENERAL DE MARINA, mayo 2002. *El Cuartel General Marítimo Español de Alta Disponibilidad-HRF (M) SP HQ.*

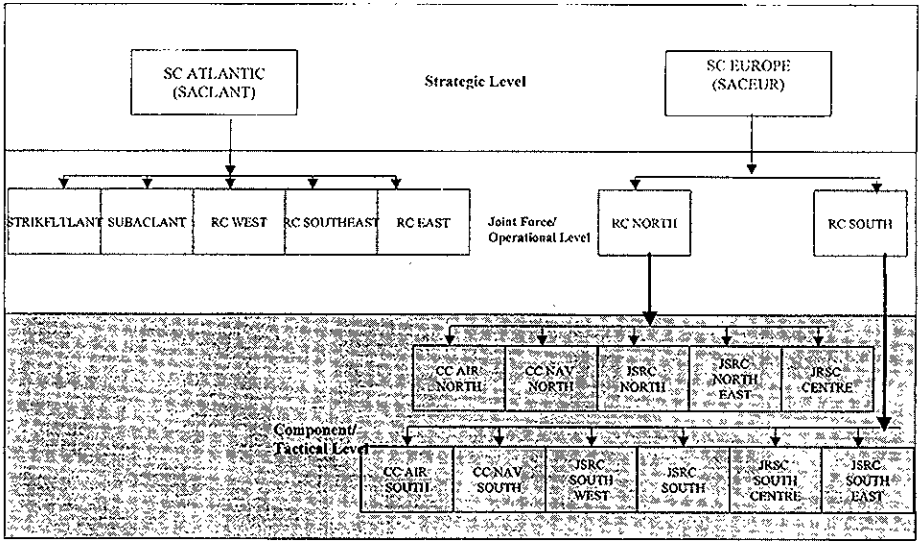


Figura 3. Estructura Estática de Mando OTAN.

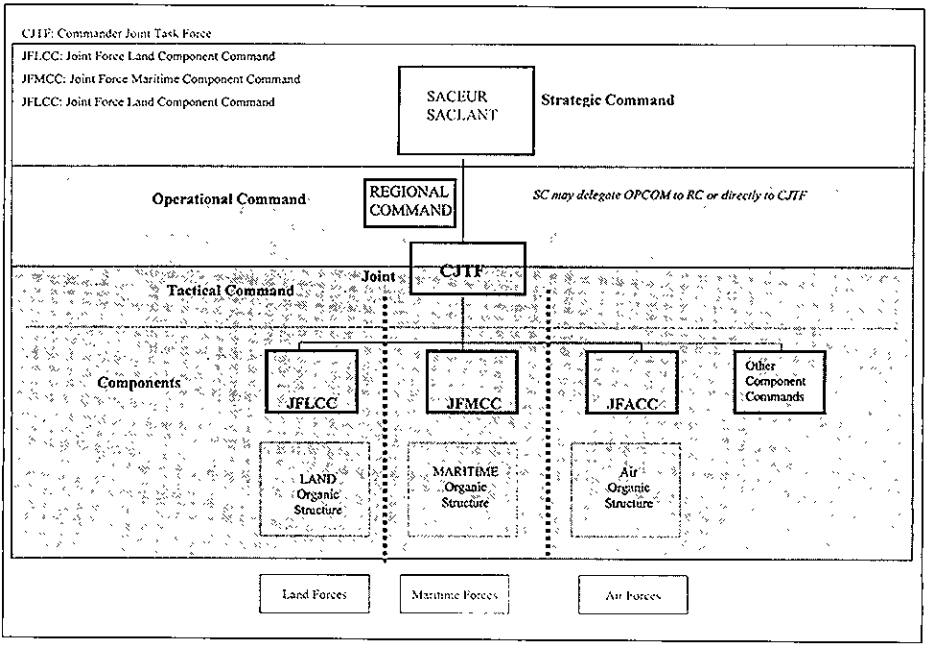


Figura 4. Ejemplo de Estructura de Mando OTAN CJTF.

Utilizando estos parámetros junto con los componentes fundamentales del SMCM, en la figura 5 se indica el marco donde encaja la Estructura Operativa de los SMCM.

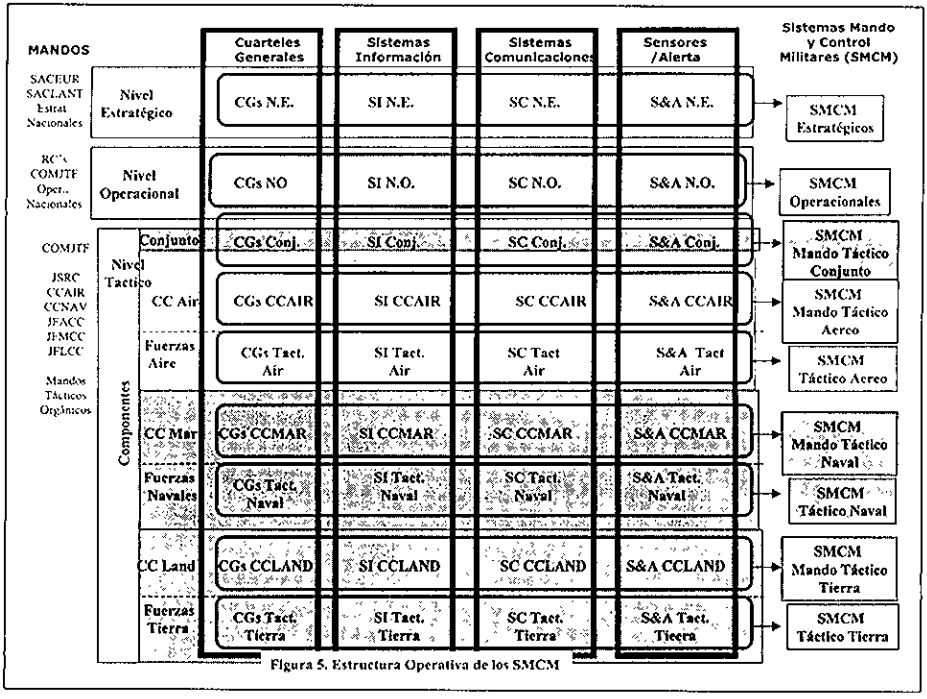


Figura 5. Estructura Operativa de los SMCM

Qué ha cambiado después del 11-S

Percepción de un nuevo tipo de amenaza

Está claro que esa fecha constituye un hito, una de esas referencias que se utilizan para separar un antes y un después. Innumerables análisis se han efectuado sobre las consecuencias del tremendo atentado terrorista a los que sólo pretendo añadir una experiencia personal. Compartía oficina en aquellos días en la agencia NC3A (NATO C3 *Agency*) con un capitán de corbeta americano, reservista, que compaginaba su destino en la OTAN con las obligadas prácticas anuales en la Marina norteamericana, y al que llamaremos Mike, por ejemplo. Mike recibió un e-mail urgente: *One of the Twin Towers is collapsing. Terrorist attack.* Después vimos por la CNN el derrumbe de la otra Torre Gemela.

Mike a duras penas podía contener las lágrimas. Un cuñado suyo trabajaba en una de las oficinas del rascacielos convertido en el informe amasijo de ruinas humeantes. Y además, ellos, *the winners*, ¡estaban siendo atacados en su propio territorio!

Alguna vez habíamos tenido interesantes conversaciones, favorecidas por ese lazo que se establece de inmediato entre oficiales de marina de cualquier nacionalidad. Yo era más antiguo e infinitamente más viejo, así que Mike me trataba con cierta deferencia.

En uno de estos intercambios entre amigos, Mike me había dicho claramente: «Mira, José, si nosotros le hacemos la guerra al resto del mundo, ganamos».

Y de repente, ¡iban perdiendo en su casa! Mascando las palabras, Mike lanzó una advertencia que se hizo realidad a corto plazo: *José, you're gonna see a lot of misiles flying around.* Y bien que los hemos visto volar.

Esta pequeña experiencia personal, me sirve para ilustrar, sin profundos análisis, lo que considero hechos fundamentales derivados del 11-S y sus consecuencias inmediatas en Afganistán e Irak:

1. La percepción de la amenaza ha completado su trayectoria desde el comienzo de la Guerra Fría:

   a) Pacto de Varsovia (durante toda la Guerra Fría).
   b) Amenaza «difusa multilateral» (desde la caída del Muro hasta el 11-S).
   c) Terrorismo internacional (después del 11-S).

2. En paralelo con la evolución de la percepción de la amenaza, tratan de adaptarse las organizaciones militares internacionales:

   a) OTAN, Artículo 5, máxima prioridad para defensa del territorio de agresiones potenciales procedentes del Pacto de Varsovia.
   b) OTAN operaciones fuera de área, no Articulo 5, para enfrentarse con difusas y variopintas amenazas.
   c) ¿Otra OTAN? ¿Defensa Europea? ¿Grupos «Rumsfeld» de alianzas temporales y *ad-hoc*, *case-to-case?*

3. Determinación de Estados Unidos a enfrentarse con la amenaza terrorista de forma sistemática y completa (hojas de ruta o *road maps*).
4. Disensión intraeuropea con dos claras actitudes:

   a) Aceptación de la hegemonía militar americana, con intención de reconducirla-moderarla desde dentro.
   b) Impulso de una suficiencia militar europea independiente de la americana.

No es mi intención entrar con este artículo en juicios de valor o análisis de intenciones, terreno difuso y apasionante. Me limito a una aproximación fáctica. Después del 11-S, el terrorismo internacional se convierte en la amenaza de las democracias. Las organizaciones militares intentan adaptarse/crearse, con discrepancias notables, pero siempre desde la colaboración multinacional.

Definición de terrorismo

Uno de los problemas de la acción contraterrorista es la delimitación clara de su definición. Como dice un autor, el terrorismo es como la pornografía, no sé definirla, pero sé qué es cuando la veo. Existen definiciones del Departamento de Defensa americano, del Departamento de Estado, del FBI, de la CIA, etcétera.

Los expertos sobre el tema han identificado un mínimo de seis tipos diferentes:

— Terrorismo nacionalista (IRA, grupos kurdos, grupos chechenos...).
— Terrorismo religioso (al-Qaeda, Hamas, extremistas judíos Kahane y Baruch Goldstein...).
— Terrorismo apoyado por el Estado *(rogue states).*
— Terrorismo de extrema izquierda (Baader-Meinhof, Brigadas Rojas...).
— Terrorismo de extrema derecha (neonazis).
— Terrorismo anarquista (GRAPO...).

No es éste el lugar para extenderse en tan importante tema, pero intentaré delimitar cuatro elementos fundamentales que subyacen como denominador común en cualquier tipo de acción terrorista:

— Es premeditada, planeada de antemano, a diferencia de un acto impulsivo de ira.
— Es política en el sentido que intenta cambiar el orden político existente, a diferencia de la violencia de grupos criminales, cuyo objetivo suele ser la consecución de dinero y riquezas.
— Sus blancos son numerosísimos y de difícil catalogación, tanto personas como edificios, monumentos, instalaciones, etc. Una característica que se busca es que tengan cierta relevancia, de la naturaleza que sea, para que atraigan la atención mediática, y de esta forma su «causa» sea conocida.
— Se efectúa por subgrupos irregulares, nacionales y/o internacionales, no encuadrados en el ejército de un determinado país.

Qué requisitos tecnológicos se derivan de la lucha antiterrorista

El fenómeno terrorista implica una adaptación de las estructuras militares, tanto nacionales como internacionales, lo que conlleva una investigación sobre procedimientos y material.

La Research and Technology Organization (RTO) de la OTAN patrocinó un taller *(workshop)* en febrero de 2002 en Arlington, Virginia (Estados Unidos) sobre el tema (6).

De los primeros análisis se encontró que existían una serie de deficiencias y limitaciones *(shortcomings and constraints)* que dificultaban la creación de escenarios de planificación. Citemos, entre otros:

a) No existe una definición formal de requisitos OTAN. En el marco nacional la situación es semejante, ya que tales requisitos no están articulados más allá de afirmaciones generales.
b) Aparte de la falta de requisitos, el contexto político está evolucionando (ver *Percepción de un nuevo tipo de amenaza*).
c) Existe una gran variedad de factores no-técnicos de gran importancia en el combate al terrorismo: consideraciones sociológicas, estatus económico, fuerzas y debilidad de infraestructuras, guerra psicológica, coordinación intergubernamental.
d) Defensa no es el único actor implicado en la guerra antiterrorista. Hay otros muchos ministerios y departamentos, desde Tecnología, Transporte, Energía hasta Interior y Sanidad.

A pesar de lo anterior, se crearon cuatro áreas de trabajo, y dentro de ellas se definieron unos escenarios y unas capacidades deseables. Como resultado del análisis, se determinaron varias áreas de colaboración tecnológica. La descripción detallada de estos temas se remite al informe del RTO. A continuación se indican de forma muy esquemática.

Áreas de trabajo

— Indicación y alerta *(indications & warning)*. Para la identificación avanzada, vigilancia y seguimiento de terroristas y sus armas.
— Supervivencia y protección *(survivability & denial)*. Para impedir el acceso a blancos terroristas potenciales.
— Gestión y recuperación de actos de terrorismo *(consequence management & recovery)*. Para la protección y la recuperación de los servicios gubernamentales esenciales.

(6) RTO. *Combatting Terrorism Workshop Report.*

— Atribución y actuación contra-terrorismo *(attribution and counteraction)*. Rápida identificación de los perpetradores de un acto terrorista y apropiadas operaciones antiterroristas.

La habilidad de ejecutar una variedad de operaciones militares en respuesta a los ataques terroristas exige nuevas capacidades para su ejecución rápida, precisa y efectiva que reduzcan las bajas sufridas por las fuerzas propias y que minimicen los problemas de bajas por fuego amigo *(fratricide)*, particularmente en situaciones de captura de rehenes.

Áreas de colaboración tecnológica

1. Sensores y Biométrica *(Sensors & Biometrics)*

   a) Vehículos Submarinos Autónomos con sistemas de sensores. *(Autonomous Underwater Vehicles* —AUVs— *with sensor suites)*.
   b) Sensores para vapor, polvo, personas dentro de vehículos y compartimentos cerrados.
   c) Biodetectores a distancia.
   d) Vigilancia subterránea de túneles, alcantarillado y aparcamientos.
   e) Detección de explosivos a distancia.
   f) Biométrica (reconocimiento e identificación de voz, reconocimiento de huellas dactilares, reconocimiento de rasgos faciales).
   g) Control de accesos.
   h) Utilización de infraestructuras existentes para soportar nuevos sensores (por ejemplo, instalación de sensores biométricos o químicos en cajeros automáticos y distribución de la información a través de la infraestructura propia de comunicaciones.

2. Tecnologías informáticas

   a) Interconexión de bases de datos (policía, inmigración, militar...).
   b) Bases de datos sobre la actividades terrorista.
   c) Arquitectura NATO de Sistemas de Información para la Alerta y Atribución Rápida.
   d) Herramientas para crear una presentación Común de Información *(Common Information Picture,* CIP) (7).
   e) Algoritmos estadísticos para identificación rápida de enfermedades.

(7) Similar a la *Common Operating Picture* (COP) en el dominio militar.

f) Redes de comunicaciones y de datos de nodos, tales hospitales, farmacias, médicos, para el análisis y fusión de datos.
g) Herramientas para construcción en tiempo real de escenarios de acciones terroristas.

3. Cyberseguridad y protección (8)

a) Identificación de intentos de acceso a sistemas informáticos y mecanismos de protección.
b) Detección en tiempo real de intentos de intrusión en redes informáticas.
c) Establecimiento de redes móviles *ad-hoc*.
d) Detección de *software* dañino *(malicious sofware)*, particularmente en paquetes comerciales (COTS, *Computer-the-shelf*).

4. Soporte a los Sistema de Decisión y Mando y Control

a) Adaptación de la estructura de Mando y Control Militar a la respuesta antiterrorista.

5. Modelización y simulación.
6. Técnicas biológicas y médicas.
7. Adiestramiento.
8. Etiquetado de material.
9. Armas.
10. Protección física.

Impacto en los SMCM de lucha antiterrorista

Dominio de las operaciones contraterroristas

De todo lo dicho anteriormente se desprende como requisitos previos y fundamentales:

1. Creación de una Doctrina de las Operaciones Contraterroristas (OCT):

Procesos implicados en las operaciones contraterroristas (se trata de establecer una doctrina completa, similar a la doctrina de las operaciones militares recogida en las *Allied Joint Publications*).

(8) Una rama de la actividad terrorista ha recibido el nombre de «Ciberterrorismo». En la sociedad «interconectada» en la que vivimos los *ciberattacks* pueden causar más daño que otras formas más vistosas de terrorismo.

2. Establecimiento de una Estructura de Mando contraterrorista (EMCT).

Tanto a nivel nacional como internacional, a los tres niveles: estratégico, operacional y táctico. Se definirán los centros o entidades de todos los organismos implicados, sus funciones y el intercambio de información en su nivel más alto.

3. Establecimiento de una Estuctura de Fuerzas Contraterrorista (EFCT).

Tanto a nivel nacional como internacional se definirán los recursos de fuerza utilizables, con consideración de los condicionantes legales de cada país.

Adaptación de los SMCM actuales

Funcionalidad e interfases

Dentro del marco anterior, y para cada SMCM (ver figura 5) se definirá en forma sistemática su función (si es que existe) y sus interfases.

— Operación Contraterrorista 1 (OCT1).
— SMCM Estratégico.
— Función.
— Interfases.

Modificación de los componentes del SMCM

Una vez completado el análisis de funcionalidad e interfases, se deben adaptar o modificar convenientemente los componentes fundamentales del SMCM:

Cuarteles Generales: inclusión, si es necesario, de una celda de operaciones contraterrorismo.

Sistemas de Información

— Adaptación de programas *software* específicos de OCT.
— Bases de datos específicas de OCT.
— Sistema de presentación específicos, tales como la *Common Information Picture* (CIP).

Sistemas de comunicaciones

— Comunicaciones específicas de OCT.
— Definición o adaptación de interfases estándar para intercambio de información, tales como AdatP-3 y Data Links.

Sensores y alerta

— Sensores y sistemas de alerta específicos de OCT.

Junto con estas adaptaciones orientadas específicamente a las OCT, debe continuarse con las adaptaciones genéricas derivadas de la movilidad y multinacionalidad de las operaciones contraterroristas, tales como:

— Arquitecturas que permitan fácilmente el despliegue *(deployability).*
— Estandarización de procedimientos e intercambio de información *(interoperability).*
— Medidas de seguridad y protección de sistemas de información (protección contra ciberterrorismo).

Resumen

Los SMCM, aparte de su misión intrínseca de instrumento para ejercer el Mando y Control de las Operaciones militares, están inmersos en el nuevo contexto derivado de la actividad contraterrorista surgida como consecuencia de los acontecimientos del 11-S.

El problema es que el contexto aún no tiene unos límites claramente definidos.

Participando en los grupos de trabajo que ya existen, nacionales e internacionales, y aplicando una metodología sistemática anteriormente esbozada, es posible una adaptación de los SMCM a los nuevos requisitos.