CENTRIXS

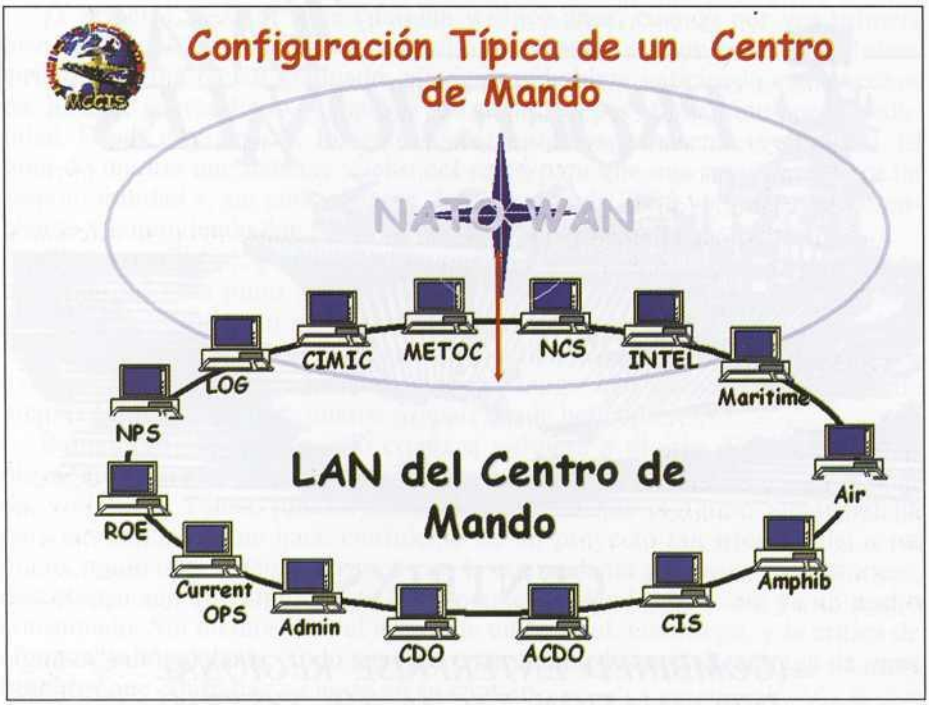
(COMBINED ENTERPRISE REGIONAL INFORMATION EXCHANGE SYSTEM)

Bernardo GONZÁLEZ SIERRA

Luis F. CALVIÑO GARCÍA

Introducción

DESDE la antigüedad el mando ha sentido la necesidad de ejercer de un modo u otro el control sobre sus fuerzas. Para ello ha usado diferentes métodos para recibir información y dar órdenes. Pero todos ellos requerían de las siguientes características: rapidez, fiabilidad, seguridad, flexibilidad y negación de esta información al enemigo. En nuestra opinión, el CENTRIXS es el paradigma de los sistemas de C2 en este nuevo siglo.



Situación estratégica actual

Hoy en día, tras los atentados del 11 de septiembre y 11 de marzo y las guerras de Afganistán e Irak, ha quedado claro que dentro de la actual guerra asimétrica el principal, y quizá el único, país con capacidad de despliegue de fuerzas en cualquier parte del mundo es Estados Unidos. Consustanciales a éstas son sus sistemas de mando y control, que son los únicos que han demostrado capacidad de unificar y comandar distintas unidades de diferentes países, integrando esas unidades en sus sistemas, logrando así la plena conectividad e interoperabilidad entre ellas. De aquí podemos deducir que sus sistemas de C2 son los más probados, los más operativos y los más interoperables.

Las razones de esta situación son variadas, y entre ellas podemos destacar:

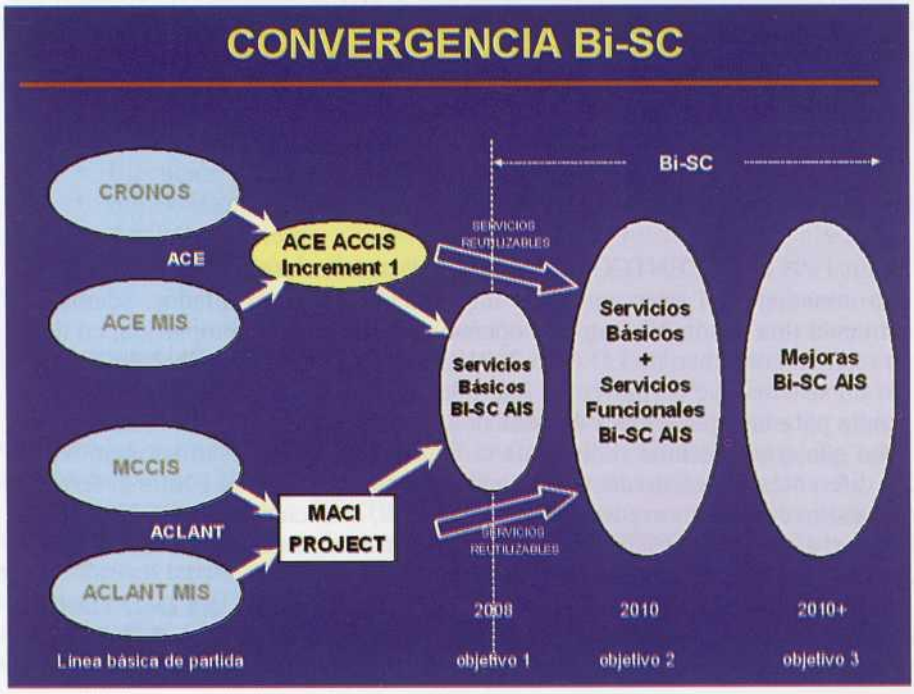
— Los Estados Unidos disponen de un presupuesto superior al del resto de los países occidentales.
— Disponen de un único criterio y unos objetivos muy claros, sin tener que satisfacer distintos intereses creados, como los que existen entre

los países de la OTAN, que ralentizan la toma de decisiones e implantación de distintos sistemas.
— Tienen una larga experiencia en operaciones en cualquier parte del mundo y con diferentes aliados, ya que prácticamente han participado en todos los conflictos después de la Segunda Guerra Mundial.
— Es impensable que la OTAN lleve a cabo una operación sin el apoyo o la colaboración de Estados Unidos.
— Las distintas alianzas para las distintas operaciones integran diferentes países, y las combinaciones de éstas y de países son ilimitadas

Sistemas de mando y control en España y la OTAN

Haciendo un repaso por los distintos sistemas de mando y control implementados en España y la OTAN, se puede ver que dentro de los ejércitos de nuestro país y de los del resto de la OTAN ha habido una evolución de estos sistemas de una manera individual, casi aislada, poniendo de nuevo de manifiesto la falta de coordinación y entendimiento entre sus distintos miembros.

En España, podemos destacar el SIJE (Sistema de Información del JEMAD) a nivel estratégico y operacional, el SIMACET (Sistema de Infor-



mación del Ejército de Tierra), el SMN (Sistema de Mando Naval), a nivel operacional y táctico, los SICOA, SMCOA y SMCFD (Sistema Informático para la Conducción de Operaciones Anfibias, Sistema de Mando y Control de Operaciones Anfibias y Sistema de Mando y Control de la Fuerza de Desembarco) dedicados a la Infantería de Marina, y el SIMCA (Sistema de Mando y Control del Aire).

En la OTAN resaltan el TARE (*Telegraphic Automated Relay Equipment*), para mensajes ACP-127, actualmente obsoleto, aunque plenamente operativo; el NCN (*NATO Core Network*), quizá uno de los mayores fiascos en cuanto a desarrollo de un sistema de mando y control, IDNX-NIDTS (*Integrated Digital Network-NATO Initial Data Transfer System*), que nacieron como sistemas *hardware* separados formando la actual *NATO Secret WAN*.

Más recientemente destacan el ACE MIS (*Allied Command Europe, Multinational Information System*) y el más conocido MCCIS (*Maritime Command and Control Information System*) para mando y control de las fuerzas terrestres y marítimas, que convergerán en el futuro BI-SC AIS (*Bi-Strategic Command Automated Information System*) junto con el ACLANT MIS (*Allied Command Atlantic Multinacional Information System*) en desarrollo actualmente y el conocido CRONOS (*Crisis Respond Operations NATO Open Systems*); este caso es curioso dado que por primera vez se intenta aglutinar varios sistemas de mando y control en uno solo con amplias capacidades. Sin embargo estos esfuerzos unificadores chocan con la reciente creación del ACCS (*Air Command and Control System*) como sistema independiente y que al parecer sustituirá al SIMCA en el Ejército del Aire. Desconocemos las razones por las que no se prevé integrarlo en el BI-SC AIS.

Breve historia del CENTRIXS

En 1999 el USCENTCOM comenzó a desarrollar este sistema con el objetivo inmediato del intercambio de información entre sus aliados, además de mantener una visión del teatro de operaciones conjunta y compartida, en tiempo real. Al comienzo de LD (año 2001) los esfuerzos se centraron en desarrollar un sistema que permitiera la interoperabilidad de la información de inteligencia para las operaciones de combate. La solución fue el CENTRIXS, pero hubo que crear distintas redes dada la gran diversidad de teatros operativos y los diferentes países aliados y coaligados dentro de la guerra contra el terrorismo; así se crearon tres redes separadas entre sí, conocidas como X-Net, GCTF (*Global Counterterrorism Force*) y MCFI (*Multinational Coalition Forces in Irak*), de las cuales se habla más adelante.

En 2002 se comenzaron a aplicar diferentes directivas del DoD (*Department of Defence*) con el fin de unificar los criterios de intercambio de información de inteligencia con otras naciones aliadas y el modo de implementar

los datos de la situación de fuerzas y orden de batalla. Este desarrollo desembocó en la necesidad de una única red global que unificara las existentes. Así en 2004 apareció como el concepto del CENTRISX-MNIS o *Multinational Information Sharing,* que llevará al sistema a ser una única red de datos común, global, multinacional e interoperable.

Servicios del CENTRIXS

Los servicios que actualmente están implementados en el CENTRIXS son mayormente COTS (*Commercial Of The Shelve*) y GOTS (*Government Of The Shelve*), sistemas comerciales o previamente desarrollados por el Gobierno, con gasto en investigación mínimo, lo que abarata enormemente su coste. Estos servicios son:

— MS INTEL OFFICE, un paquete de Microsoft Office profesional, especialmente adaptado a redes.
— *Net meeting* como herramienta de colaboración.
— Voz sobre IP.
— GCCS-I3 (*Global Command and Control System Integrated Imagery and Intelligence*), sistema GOTS que se implementa en CENTRIXS debido a sus posibilidades:

- Identificación y evaluación de la amenaza.
- Ayuda al planeamiento estratégico.
- Desarrollo de las diferentes líneas de actuación.
- Ejecución y puesta en práctica de lo planeado.
- Supervisión.
- Análisis del riesgo.
- Presentación de la situación táctica.

Estructura actual del CENTRIXS

Diez redes componen principalmente el sistema CENTRIXS, tres de ellas son globales y unen USCENTCOM-USPACOM-USEUCOM, es decir, los mandos de Estados Unidos en Oriente Medio, el Pacífico y Europa.

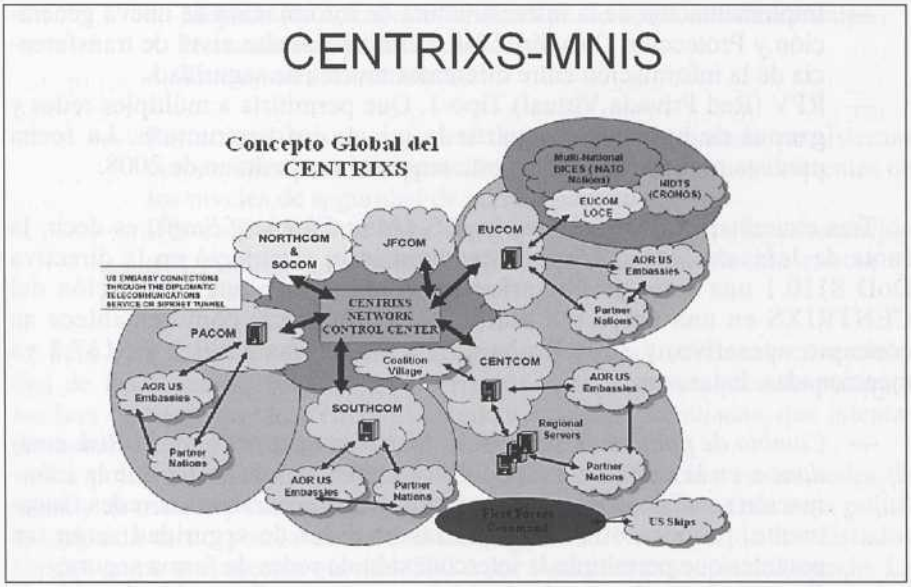
Entre las redes locales, USCENTCOM utiliza tres para su uso exclusivo con sus aliados en su área de responsabilidad, CENTRIXS-MCFI, para las operaciones en territorio iraquí, y para dar conectividad a las grandes unidades de terrestres, hasta el tamaño mínimo de una brigada, instalaciones y estados y planas mayores. CENTRIXS-GCTF, cuyo uso principal es dar conectividad a las unidades navales y a las unidades propias y aliadas sobre territorio afgano,

y X-NET, creada para dar conectividad a las grandes unidades aéreas y a los aliados pertenecientes a la Commonwealth.

Las tres redes son usadas por USPACOM para el control sobre las operaciones que se llevan a cabo en su área de responsabilidad. Son las conocidas como COWAN-J (*Coalition Wide Area Network*), COWAN-K y COWAN-T. Esta multiplicidad de redes locales es debida al distinto nivel de accesibilidad a la información de los aliados en la zona del océano Pacífico. Asimismo estas redes son usadas ocasionalmente como banco de pruebas para distintas mejoras del sistema en los ejercicios JWID/CWID (*Joint/Combined Warrior Interoperability Demostrator*).

Finalmente USEUCOM mantiene una red tipo CENTRIXS experimental, conocida por CFBLNet (*Combined Federated Battle Laboratories Network*). Aquí es donde se están llevando a cabo la mayoría de las pruebas de conectividad y seguridad que darán al CENTRIXS-MNIS sus capacidades futuras.

Uno de los desarrollos fundamentales en el programa del CENTRIXS es lo que se conoce como Griffin, el soporte físico de la red CENTRIXS. El Griffin tiene un acercamiento arquitectónico diferente a los otros sistemas actualmente en uso. Originalmente nació como una iniciativa del CCEB (*Combined Comunication Electronic Board*), pero actualmente está siendo desarrollado por las naciones del grupo MIC (*Multinational Interoperability Council*); a saber, Estados Unidos, Gran Bretaña, Australia, Canadá, Francia, Alemania y Nueva Zelanda. El Griffin está definido por el MIC como «el desarrollo permanente a nivel multinacional de los recursos y capacidades para el intercambio de la información entre las redes clasificadas de las naciones que participan». En cualquier caso, el Griffin no será la red física definitiva, pero mientras tanto proporciona ayuda para el desarrollo de muchos servicios que



serán implementados. El Griffin ayuda además a definir el concepto de dominios múltiples, donde un dominio se define como «un ambiente común donde los participantes pueden intercambiar la información de la cual se protegen contra la intrusión de no-participantes». Esto significa que una sola infraestructura puede apoyar diversas coaliciones, con naciones que participan conectándose con los dominios múltiples, si es necesario.

El CENTRIXS está pensado para formar, un día, una sola red de información común, global y multinacional. Para lograr este objetivo, es absolutamente necesario lograr una solución tecnológica que certifique la posibilidad de compartir información confidencial multinivel sobre una red frente a la actual proliferación de múltiples redes separadas. La tecnología de seguridad que permitirá comunidades de intereses, separadas pero simultáneas, a través de una red común de transporte, es la clave para el futuro de las redes de Mando y Control en el mundo.

Requisitos operativos

En mayo de 2004, el USCENTCOM envió el listado de los requisitos más necesarios a la Junta de Jefes del Estado Mayor:

— Navegación web-Integración en SIPRNET.
— *Net-Meeting/Messenger.* como herramienta de colaboración.

— Implementación de la infraestructura de información de nueva generación y Protección *One Way Link*. Permitirá un alto nivel de transferencia de la información entre diferentes niveles de seguridad.
— RPV (Red Privada Virtual) Tipo-1. Que permitiría a múltiples redes y grupos de usuarios compartir la misma infraestructura. La fecha prevista para dar solución a este requisito es el verano de 2008.

Tras examinar estos requisitos, la JCS (*Joint Chiefs of Staff*), es decir, la Junta de Jefes de Estado Mayor estadounidense, estableció en la directiva DoD 8110.1 una serie de directrices para lograr la plena integración del CENTRIXS en una única red multinivel y dinámica, como establece su concepto operativo, y se indicaba en las Directivas 8100.1 y 5137.1 ya mencionadas. Éstas son:

— *Cambio de política de seguridad*: *Risk management* frente a *Risk avoidance*, en la que frente a la política tradicional de evitar que la información sensible caiga en manos indeseadas separando las redes físicamente, propone otra en la que las medidas de seguridad serán tan potentes que permitirán la interconexión de redes de forma segura.
— *Potenciadores de tecnología*: básicamente se refiere a la adopción de *chat* y traductores simultáneos.
— *Desarrollar un ambiente seguro multinivel y dinámico*, es decir, que el tránsito de la información desde Sinclass a CTS sea por la misma red, con la adecuada protección, y que además permita conectar este sistema a cualquier otro sistema de C2 que posea cualquier otra nación para alianzas *ad hoc*.

Sin embargo, el Estado Mayor Conjunto de los Estados Unidos definió como objetivo fundamental para lograr el adecuado intercambio de la información aquel sistema que proveyera la posibilidad a cualquier miembro de la coalición de tener acceso inmediato a la información susceptible de ser compartida. Así, el Estado Mayor Conjunto norteamericano hizo las siguientes recomendaciones específicas:

1. Cambio de la actual política/filosofía de seguridad.
2. Potenciar el intercambio de información con países extranjeros.
3. Educar al usuario en las políticas nacionales de acceso a la información y sus procedimientos de implementación.
4. Mejorar la implementación de la política de seguridad:

— Racionalizar el proceso de acceso a la información de los extranjeros.
— Racionalizar y estandarizar las políticas de los sistemas de seguridad.
— Integrar potenciadores de tecnología:

- Mejorar los actuales estándares de las redes multinacionales.
- Herramientas para la colaboración.
- Traductores simultáneos.

— Permitir el uso de *software* de encriptación basado en sistemas comerciales para la separación de grupos de usuarios diferentes en los niveles de seguridad de secreto para abajo.
— Desarrollar un ambiente seguro y multinivel para la información que permita a los aliados, el acceso a la información exacta en base a su necesidad de conocer.

Pero para lograr estos objetivos hay que superar la tradicional vulnerabilidad de las redes no sólo a ataques físicos, sino a los ataques de posibles *hackers* de naciones tanto enemigas como eventualmente aliadas, que intentaran hacerse con algún tipo de información clasificada.

La política tradicional para salvaguardar la información en las redes de datos y de mando y control ha sido la de «evitar los riesgos». Ésta es la política seguida tanto por la autoridad de Seguridad Nacional de los Estados Unidos como por nuestro querido CNI o por cualquier potencia del mundo. La historia nos demuestra que ante la inseguridad que suponen los ataques informáticos, la mejor manera de proteger la privacidad, integridad, disponibilidad y autenticidad de nuestra información siempre ha sido conectar en la red el número mínimo de ordenadores, a los que sólo tengan acceso aquellas personas con necesidad de conocer, evitando que en la red participen personas o grupos que no deban compartir la información y/o los datos que en esa red se vuelcan. Sin embargo, el mismo concepto del CENTRIXS-MNIS hace que no sea posible seguir llevando a cabo esta política.

Medidas de seguridad

Implantación de los algoritmos dinámicos de cifrado

Simplificándolo mucho, es la selección de modo pseudoaleatorio de un algoritmo de cifrado de una batería de éstos.

Ultra Thin Client

Se trata básicamente de que sólo se pueda acceder tanto a determinadas aplicaciones como a los datos que éstas manejan desde equipos autorizados e identificados por su propia tarjeta de red, así como por otros métodos.

Relleno del tráfico

No es más que la producción continua de *bits* con el objeto de que si alguien se encuentra grabando o escuchando en una línea sea incapaz de saber cuándo se está transmitiendo verdadera información y cuándo simple ruido.

Cifrado de clave pública (PKI), common access card (CAC) e identificadores de parámetros biométricos

El cifrado por clave pública se basa en funciones matemáticas en lugar de operaciones sobre patrones de *bits*, como se realiza con los algoritmos de encriptación tradicionales. El núcleo de este sistema son los algoritmos de cifrado y descifrado, así como las claves pública y privada utilizadas bien para cifrar o descifrar. Este sistema sirve además para autentificar la información por el procedimiento de la firma digital. Para complementar y facilitar el uso de la clave pública se está implantando la tarjeta de identificación de acceso común, en la que parte de la clave privada estará contenida en un chip dentro de una tarjeta de identificación.

Además se implementarán identificadores de parámetros biométricos para comprobar las huellas digitales del usuario o lectores de retina, etc., que verificados contra un servidor darán acceso a la información.

IPSec en IPv6

El Departamento de Defensa de los Estados Unidos lleva años utilizando Internet para el envío de información hasta el nivel de seguridad de CONFIDENCIAL. Esto es así a través de la conocida como SIPRNET, que implementa comunicaciones seguras sobre IP y el protocolo HTTPS en los niveles de red y sesión. Estos servicios fueron pensados para ser aplicados en IPv6, aunque compatibles con la actual versión de Internet IPv4.

Entre las aplicaciones se incluyen:

— Conectividad segura entre usuarios a través de Internet.
— Acceso remoto seguro a través de Internet.
— Establecimiento de conectividad Intranet y Extranet con socios de una comunidad de interés.

Además IPSec proporciona servicios de encriptación similares a la PKI. Por todo lo anteriormente reseñado, el CENTRIXS alcanzará su máxima grado de operatividad cuando el uso de IPv6 se generalice, alcanzando grados de control sobre la fuerza que hoy sólo vemos en películas de ciencia ficción.

Trusted sessions managers

Ésta es la tecnología que permitirá la gestión de todos estos elementos de seguridad. Actualmente es la menos desarrollada y es, en último lugar, lo que estará retrasando la implementación a escala mundial del CENTRIXS.

Dos tecnologías están siendo desarrolladas para el CENTRIXS: el *Multi-Level Session Server* (MLSS) y el DODIIS *Trusted Workstation* (DTW). Ambas están basadas en Solaris. El MLSS permitirá básicamente que un grupo se conecte de modo seguro a un servidor de un determinado nivel de seguridad, restringiendo además el almacenamiento de información a los servidores, proveyendo a los usuarios finales con discos duros portátiles y asegurando una apropiada limpieza de los *buffers* de memoria y memorias caché entre las diferentes sesiones o conexiones a la red; así los usuarios podrán acceder a los diferentes servidores de CENTRIXS.

El DTW será utilizado para proporcionar a un usuario acceso simultáneo a diversos enclaves de almacenamiento de información del CENTRIXS, mientras que previene la posible pérdida de la información entre estos enclaves.

Conclusión

Éste es el sistema C2 por el que, en mi opinión, debería apostar tanto la Armada como el Ministerio de Defensa, como ya han hecho países como el Reino Unido, Alemania o Francia.

Tanto por su concepto como por el uso de aplicaciones y sistemas de desarrollo comercial, y por la solidez y robustez de los sistemas de seguridad a implantar, esta red de mando y control podrá ser implementada a través de la red física de la Internet tradicional de alta velocidad (ADSL, XDSL, cable, WIMAX, ATM, etc.), lo que aumentará de manera inusitada la versatilidad de esta red de mando y control, pudiendo llegarse, quizá, a ejercer determinadas actividades del mando y de las operaciones militares desde prácticamente cualquier lugar, incluido el mismo domicilio, aumentando aún más el concepto de disponibilidad y flexibilidad del militar en cualquier momento y ocasión.

BIBLIOGRAFÍA

Department of Defence Instruction N.º 8110.1 *Multinational Information Sharing Networks Implementation*, de 6.02.2004.

US Department of Defence Directive N.º 8100.1 *Global Information Grid* (GIG) Overarching Policy de 19.09.2002.

US Department of Defence Directive Nº 5731.1 Assistant Secretary of Defence for Command, Control, *Communications and Intelligence* (ASD C3I) de 12.02.1992.

Combined Enterprise Regional Information Exchange System (CENTRIXS); Supporting Coalition Warfare World-wide. Jill L. Boardman and Donald W. Shuey.

Acta del ITP (*Interoperability Test Panel*, US DoD) del 30.01.05.

Project Budget Justification US Navy FY 04, 05, 06 and 07.

BAUMAN, Dennis L.: *Decision Superiority for the Joint War Fighter*.

BARRY, Charles L.: *Transforming NATO Command and Control for Future Missions*.

Operation Tiki-II, Impact of New Communication Systems.

STALLINGS, William: Comunicaciones y Redes de Computadoras (Pearson-Prentice Hall) 7.ª Ed. *www.usaarl.army.mil*

HUIDOBRO MOYA, José Manuel: *Redes y Servicios de Telecomunicaciones* (Paraninfo) 1.ª Ed.

A. NATO Perspective on CENTRIXS, NC3Board (L. Parker).