CD&E: Ciberdefensa Táctica

Cte. Javier Bermejo Higuera,
Cap. Fernando Llorente Santos,
Área TICS, ITM

Palabras clave: ciberdefensa, experimentación, mando y control

Metas tecnológicas relacionadas: MT 6.4.4.

En la actualidad, la mayoría de los sistemas de mando y control e información militar, así como determinados sistemas de combate y de control de plataformas y armas, están conectados a través de redes militares de comunicaciones que, en mayor o menor medida, también están expuestos a las diferentes amenazas que existen en el ciberespacio: disponen de interconexiones a otros sistemas, ya sean OTAN, UE o de países aliados; forman parte de una federación de redes en el ámbito operativo; o sus enlaces se realizan en ciertas ocasiones a través de infraestructuras civiles, lo que complica el establecimiento y mantenimiento de la seguridad.

Además, la futura adaptación de estos sistemas al concepto NEC *(Network Enabled Capability)* incrementará la capacidad de mando y control de los ejércitos. Las nuevas plataformas aéreas ya disponen de sistemas de comunicaciones para recibir y transmitir información constantemente; los sistemas de defensa aérea son teleoperados por ordenador; los sistemas de inteligencia, vigilancia y reconocimiento (ISR) recogen tanta información que el desafío está en obtener los datos críticos; las unidades de infantería disponen de sistemas de comunicación de banda ancha, sistemas de posicionamiento (FFT, *Friendly Force Tracking)* y dispositivos de visión nocturna, en todos ellos existen dispositivos de proceso que representan una fortaleza pues incrementan la capacidad de combate, pero que también podrían convertirse en una debilidad pues presentan vulnerabilidades, lo que exige la adopción de medidas para su protección, con la consecuente y necesaria puesta en marcha de capacidades de ciberdefensa.

Para obtener una radiografía del estado de ciberdefensa en el entorno táctico, nació un proyecto de desarrollo y experimentación de conceptos (CD&E) en la Dirección de Investigación, Doctrina, Orgánica y Materiales (DIDOM) del Mando de Doctrina (MADOC) del Ejército de Tierra. El objeto de este ejercicio consiste en analizar, mediante la experimentación, el estado de los sistemas CIS desplegables del Ejército, proponer y validar soluciones de mejora, así como extraer las enseñanzas, mediante la fase de análisis de los datos capturados durante la realización del mismo, que sirvan para depurar estas soluciones y elaborar una guía de recomendaciones útiles que incrementen sus capacidades y su eficacia en el uso del ciberespacio.

Dentro del marco del proyecto, se incluía la ejecución de un experimento de objetivo limitado (LOE) de ciberdefensa en el marco de un escenario virtual, que simule un posible despliegue de una brigada con apoyos de guerra electrónica, con todos los sistemas CIS desplegables del Ejército, como pueden ser el SIMACET, TALOS, GESTA, FFT, etc. El ejercicio tuvo lugar en las instalaciones del

Área TICS del Instituto Tecnológico La Marañosa (ITM) entre los días 10 al 14 de diciembre de 2012, con amplia representación tanto de personal experto en ciberdefensa desde su aspecto técnico, como con respecto a sus repercusiones en aspectos legales, políticos, sociales y económico-empresariales.

En el mismo han participado organismos de Defensa como el MADOC, REW31, RT22, BRITRANS, DIVOPE, JCISAT, PCMHS, CIFAS, ISDEFE, ITM-TICS; de la Administración Pública como

Fig. 1. El General del ITM recibe al General de DIDOM.

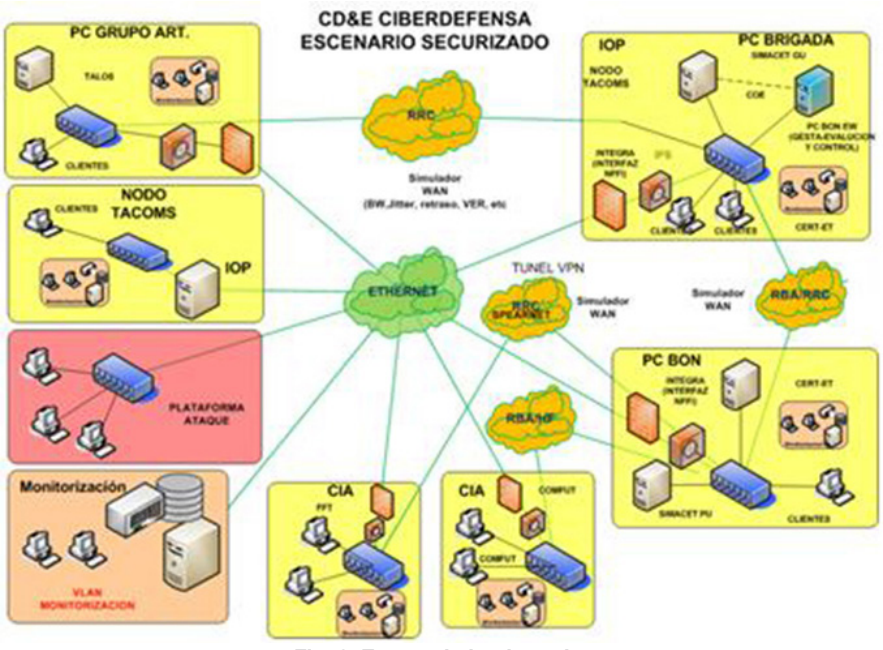

Fig. 2. Escenario implantado.

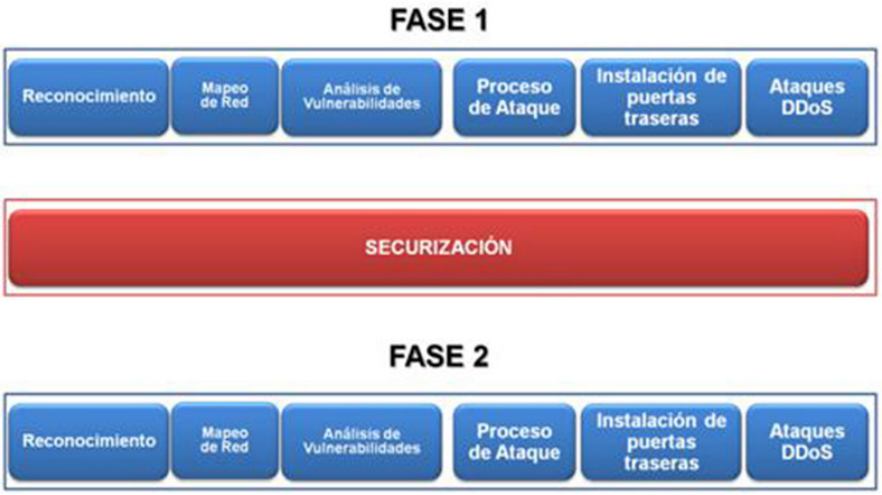

Fig. 3. Diagrama de fases.

CNPIC (Centro Nacional para la Protección de Infraestructuras Críticas) o INTECO, la Unidad Central Operativa de la Guardia Civil; periodistas de Asociación de Prensa de Madrid, ATENEA e INFODEFENSA; empresas privadas S21SEC, INNOTEC, CIDITES, INDRA; expertos en jurisprudencia y representantes de la academia como la Universidad de Granada y de la de Oviedo.

El ITM, y en particular su área TICS, realizó el apoyo tecnológico a la experimentación del concepto de ciberdefensa militar a petición del mando del MADOC. Dentro de este proceso se han llevado a cabo las reuniones pertinentes para la definición y elaboración de los distintos documentos, como el de "Concepto de Ciberdefensa Militar del ET", base del proyecto CD&E en donde se plantea el problema a resolver, así como el "Documento de Descripción del Proyecto (DDP)", donde se planifica el alcance y desarrollo del concepto y del experimento que lo apoya, del "Documento de Diseño del Experimento (DDE)", donde se explican detalladamente los aspectos relativos a la realización del experimento.

Para la preparación del evento se dispusieron de dos entornos de trabajo en paralelo, uno que albergaba la Plataforma de Ataque y otro en el que se emplazaron los sistemas tácticos de mando y control SIMACET (batallón y brigada), COMFUT, FFT, TALOS, GESTA y TACOMS interoperando a través de la herramienta INTEGRA del IT M, así como el CERT *(Computer Emergency Response Team)* desarrollado por JCISAT.

Se dividió el ejercicio en dos fases en las que se seguía una metodología de ataque idéntica en cada una de ellas: mapeo de red; análisis de vulnerabilidades; proceso de ataque; instalación de puertas traseras y ataques de denegación de servicio, pero estableciendo en la segunda medidas de seguridad específicas desarrolladas por la Unidad de Seguridad del Área TICS, para mejorar y securizar el entorno táctico de mando y control. También se establecieron una serie de métricas para poder evaluar de forma cuantitativa la mejora del nivel de seguridad entre las dos fases.

Por otra parte se desarrolló un escenario ficticio en el que se planteaban distintas incidencias de seguridad desde aspectos diferentes al técnico y que pueden influir en la vulnerabilidad de los sistemas tácticos de mando y control desplegados en zona de operaciones, con el propósito de recabar la opinión de expertos en la materia y determinar su influencia en el éxito de las misiones encomendadas al Ejército. La infraestructura empleada para el evento fue la siguiente:

- Dos salas de trabajo, con los ordenadores necesarios para recrear las plataformas de ataque y los sistemas tácticos C2 desplegados.
- Infraestructura virtual de soporte compuesta por varios servidores físicos y alrededor de sesenta máquinas virtuales, un puesto de control y un equipo de dos personas proporcionando soporte técnico.
- Una infraestructura de recolección de información independiente en cada una de las áreas de trabajo para conocer qué sucesos estaban produciéndose.
- Una sala de reuniones para la revisión y recapitulación de lo acontecido durante cada jornada de trabajo.
- Una sala con doce puestos de recolección de información mediante cuestionarios orientados a recabar el estado de las capacidades de ciberdefensa actualmente desplegadas en los distintos organismos participantes y su relación con los controles de seguridad específicos implantados en cada uno de ellos.
- Una sala de discusiones dirigidas para la participación abierta de expertos en la materia.
- Un puesto de red Wi-Fi e Intranet de Defensa en cada sala para acceso y consulta de información externa.

Fig. 4. Sala de equipos de atacantes.

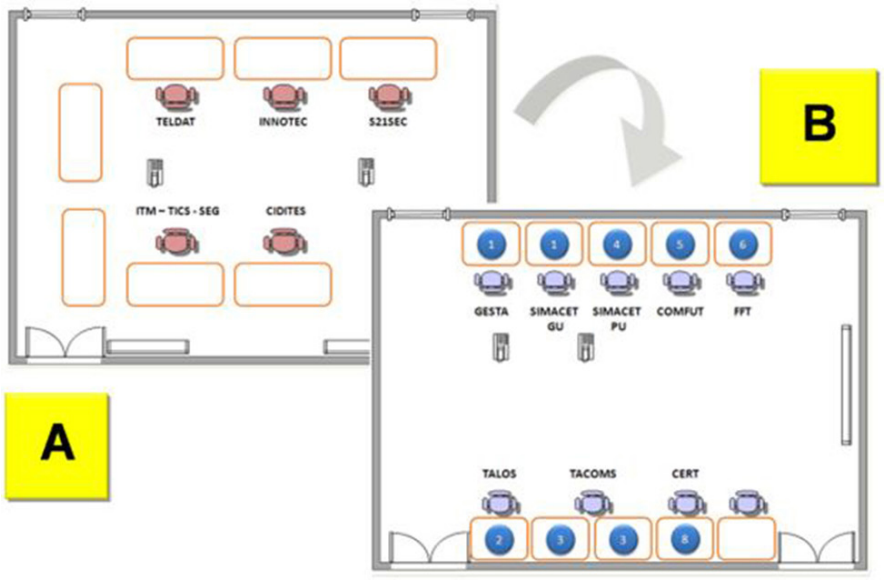

Fig. 5. Disposición de los equipos de trabajo.

El ITM, para la preparación y ejecución del ejercicio, tuvo que realizar las siguientes actividades:

- Descripción del proyecto CD&E y diseño del experimento: 8 semanas.
- Preparación de la infraestructura virtual para la realización del experimento: 8 semanas.
- Desarrollo de la plataforma de recolección y análisis de datos: 3 semanas.
- Desarrollo de la aplicación de gestión y recolección de información del evento.
- Preparación y pruebas del entorno de experimentación del evento.
- Participación como responsables de la recolección y análisis de la información: 8 semanas.

En la actualidad, el ITM está finalizando la fase de análisis del experimento. A modo de resumen el experimento se estructuró de la siguiente forma:

- Dos fases de ataque, una sin securizar el entorno de sistemas de mando y control y otra con el entorno securizado.
- Se delimita el tiempo de realización de ataques en cuatro días (El número que mencionaron los representantes del CERT (Centro de Emergencias y Respuesta Temprana).
- Cuatro sesiones de reuniones de expertos en distintas disciplinas para estudiar el problema de la ciberdefensa desde otros aspectos como el social, político, económico y militar. Para ello se presentó un escenario con distintas incidencias para que los expertos en estos campos pudieran debatir libremente en cuatro sesiones de discusiones dirigidas que se plantearon.
- Tres cuestionarios (Demográfico; Controles vs . Capacidades ; Desarrollo de las sesiones) con sesenta preguntas en total.
- Un registro de los eventos que se estaban produciendo.

La sesión final del día 14 fue dedicada a la presentación de las “primeras impresiones” del experimento por parte de los distintos implicados.

Fundamentalmente se presentaron las conclusiones cualitativas alcanzadas, a expensas de realizar un análisis cuantitativo exhaustivo de los datos recogidos en las diferentes jornadas, que se pueden resumir en los siguientes puntos:

- Se considera de gran importancia la aplicación de las guías STIC (Sistemas y Tecnologías de Información y Comunicaciones) del CCN (Centro Criptológico Nacional) a los sistemas y actualización de su software de base (sistemas operativos, sistemas gestores de bases de datos, etc.) al objeto de que sean más resistentes a los ataques y no sean tan dependientes de las medidas de protección de red (cortafuegos, detección de intrusiones, etc.).
- Potenciar la formación en ciberdefensa tanto a nivel de los administradores, operadores de sistemas y personal de seguridad incluyendo las capacidades de respuesta y fomentar la concienciación e implicación en ciberseguridad de todo el personal destinado en zona de operaciones.
- Se considera necesario la capacidad de disponer de un CERT desplegables con capacidades de detección y monitorización de ciberataques, tal y como ya lo tiene implementado el Ejército de Tierra.
- Necesidad de implantar en el ITM un laboratorio que verifique, valide y certifique la seguridad de los sistemas TIC del Ministerio de Defensa en lo relativo al *hardware* y al *software*. Actualmente ya se disponen de capacidades auditoras de seguridad de código fuente de software.

Fig. 6. Sala de encuestas y recogida de información.

- Importancia de desarrollar un sistema de ofuscación *Honey Net* (redes trampa) como medida para incrementar la seguridad de los sistemas y detección de patrones de ataques. Actualmente el ITM está desarrollando una, en la que se incluye una línea de investigación de detección de patrones de ataque basado en ontologías.
- Impulsar la celebración de una serie de futuros LOE de sistemas específicos dentro del dominio de la Ciberseguridad. En este sentido, se ha propuesto a primeros de año la realización de uno con la nueva versión del Sistema de Mando y Control del Ejército SIMACET 4.01.
- Se ha comprobado la vulnerabilidad de los sistemas a uno de los ataques de denegación de servicio distribuido (DDoS), usados masivamente en los ataques a Estonia y Georgia en 2007 y 2008 respectivamente.
- Los procesos CD&E constituyen una magnífica iniciativa que permite aprender de las experiencias vidas y mejorar en función de ese aprendizaje. El valor añadido en el realizado, es el examen de los sistemas C2 sometidos a la operación de actores reales, con herramientas y perfiles de atacante que son los que se encuentran en el ciberespacio.

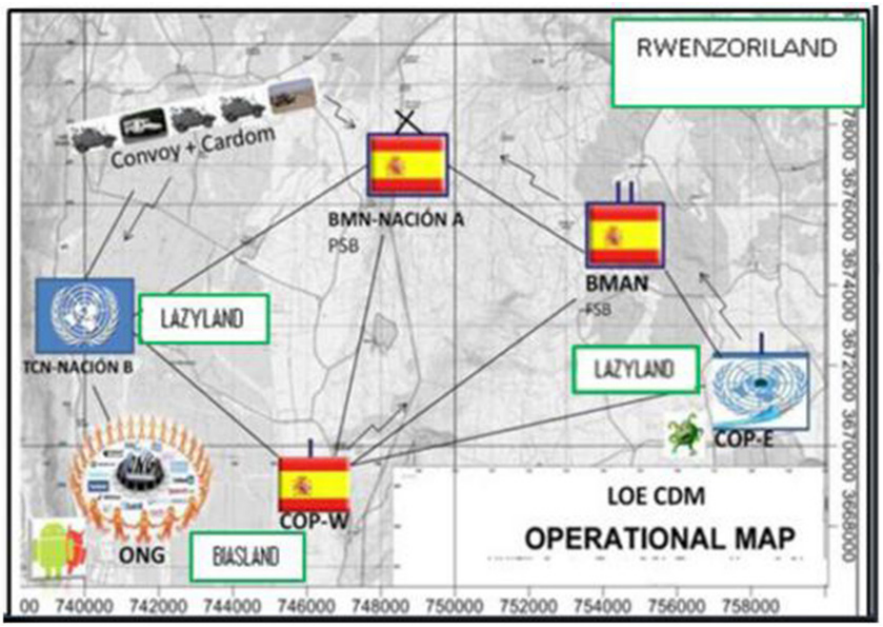

Fig. 7. Escenario de incidencias.

Fig. 8. Mesa de debate de percepción del medio.

enlaces de interés

La Subdirección General de Tecnología e Innovación ha puesto en marcha los espacios colaborativos del Portal de Tecnología e Innovación del Ministerio de Defensa.

Estos espacios surgen con el objetivo de fomentar el intercambio de información y el trabajo colaborativo entre los diferentes actores de la I+T de Defensa, facilitando que los distintos usuarios puedan compartir sus opiniones e ideas sobre las nuevas tecnologías y soluciones innovadoras de aplicación a defensa.

Para acceder a los espacios colaborativos es necesario registrarse en el sistema. Esto se realiza a través de la opción “Registro en el sistema” del menú “Contacto y participación” de la página principal del Portal de Tecnología e innovación del Ministerio de Defensa www.tecnologiaeinnovacion.defensa.gob.es o directamente a través del siguiente enlace:

www.tecnologiaeinnovacion.defensa.gob.es/eses/Contacto/Paginas/Registro.aspx