DOCUMENTO INFORMATIVO DEL IEEE 09/2011

NUEVO CONCEPTO DE CIBERDEFENSA DE LA OTAN

(MARZO DE 2011)

1. INTRODUCCIÓN

El pasado 10 de marzo los Ministros de Defensa de la OTAN aprobaron el Nuevo Concepto de Ciberdefensa de la Alianza. Este concepto define la protección de las redes de la OTAN como una responsabilidad fundamental de los aliados.

También se destacó la importancia de cooperar con sus socios y otros organismos internacionales en ciberdefensa, y la necesidad de integrar las ciberamenazas en el planeamiento de defensa de la OTAN. Se espera que los ministros de Defensa aprueben una revisión de la Política de Ciberdefensa y una Acción de Ciberdefensa en la próxima reunión de junio.

Durante la reunión, los Ministros de Defensa comprobaron el progreso de un conjunto de medidas que se decidieron en la Cumbre de Lisboa del pasado mes de noviembre de 2010 para conseguir que la Alianza sea más efectiva y eficiente a la hora de abordar las nuevas amenazas a la seguridad.

2. CONTEXTO Y EVOLUCIÓN

Aunque la OTAN siempre ha protegido sus sistemas de información y comunicaciones, la Cumbre de Praga de 2002 incluyó esta función en su agenda política. En la Cumbre de Riga de 2006 los aliados reiteraron la necesidad de proteger los sistemas de información propios de la organización.

Los ciberataques a Estonia en la primavera de 2007 marcaron un hito y un reto histórico para la OTAN [1]. Fue la primera vez que un país miembro solicitó apoyo a la OTAN por un ataque a sus sistemas de información y comunicaciones. En aquel momento la OTAN no disponía de un plan de acción para el caso de un ciberataque a un Estado miembro. En la reunión de junio de 2007 los ministros de Defensa acordaron trabajar urgentemente sobre este tema. En un informe de octubre de ese mismo año[2] la OTAN recomendaba la implementación de un conjunto de medidas orientadas a mejorar la protección ante los ciberataques. También se acordó desarrollar una Política de Ciberdefensa.

[1] Para más información véase el capítulo IV del Cuaderno de Estrategia nº 149 "Ciberseguridad. Retos y
[2] Report of the examination of the lessons learned from the recent cyber attacks", -AC/322-D(2007)0050 - 01.10.2007

Los ciberataques continuaron evolucionando rápidamente en frecuencia y complejidad, como demostraron los casos de Lituania y Georgia en julio de 2008 y el ciberataque a Kirguistán en enero de 2009. La guerra de Georgia del verano de 2008 demostró que los ciberataques eran un componente más de los conflictos.

La OTAN se enfrentó a este problema en la Cumbre de Bucarest de 2008, de cuya declaración se desprendían tres líneas de acción que consistían en medidas a adoptar:

- por la propia OTAN para mejorar su capacidad de ciberdefensa
- por las naciones para mejorar la protección de los sistemas de información crítica desplegados en sus territorios y
- por ambas partes, OTAN y naciones, para mejorar la coordinación, intercambio de información y el apoyo mutuo.

Entre las medidas adoptadas por la OTAN para mejorar sus capacidades de ciberdefensa, el Consejo de la OTAN firmó la Política de Ciberdefensa en enero de 2008[3] con el objetivo de mejorar la capacidad de la OTAN para proteger los sistemas de información y comunicaciones de importancia crítica para la Alianza frente a los ciberataques; desarrolló el concepto de ciberdefensa[4]; aceleró el proceso para conseguir una capacidad operativa completa de respuesta ante incidentes informáticos-NCIRC[5].

Tanto el Nuevo Concepto Estratégico como la Declaración de la Cumbre de Lisboa inciden en que la protección de los sistemas de información y comunicación de la Alianza es una tarea urgente de la que depende el futuro de la seguridad.

En concreto, la Cumbre de Lisboa ordenó el desarrollo de una nueva Política de Ciberdefensa y un Plan de Acción para finales de junio de este año[6].

La OTAN utilizará los procesos de planeamiento de la defensa para promover el desarrollo de las capacidades de ciberdefensa de los aliados, para ayudar a las naciones aliadas que lo soliciten y para optimizar la compartición de información, la colaboración y la interoperabilidad.

Para tratar las amenazas a la seguridad que provienen del ciberespacio, la OTAN trabaja con otros actores como Naciones Unidas y la Unión Europea.

[3] "NATO Policy on Cyber Defence", C-M(2007)0120.
[4] "NATO Cyber Defence Concept, MC 0571, 4-2-2008.
[5] NATO Computer Incidents Response Capability Technical Centre – NCIRC. Este centro consta de un centro de apoyo y coordinación de ciberdefensa y de un centro técnico que serían como el NATO CERT.
[6] Durante la apertura de una reunión celebrada en enero con representantes de las naciones para estudiar cómo impulsar la cooperación multinacional en el área de ciberdefensa, el embajador Gabor Iklody, Secretario General Adjunto para Desafíos Emergentes de Seguridad dijo: "A partir del compromiso de Lisboa de capacidades críticas y del nuevo concepto estratégico de la OTAN, la nueva Política de Ciberdefensa y el Plan de Acción de junio tratarán dos cuestiones principales: ¿qué queremos defender? Y ¿cómo queremos defenderlo?".

3. PRINCIPALES ACTIVIDADES DE CIBERDEFENSA

La OTAN realiza en este ámbito actividades de: coordinación y asesoramiento en ciberdefensa; asistencia a las Naciones; investigación y formación; y cooperación con los socios.

Coordinación y asesoramiento en ciberdefensa

La política de ciberdefensa se implementa mediante las autoridades políticas, militares y técnicas de la OTAN, así como por las naciones. La Autoridad para la Gestión de Ciberdefensa-CDMA[7] es la responsable de la coordinación de este ámbito dentro de la Alianza, centrándose particularmente en la amenaza cibernética; la gestión del riesgo de seguridad; la valoración de las vulnerabilidades; y la continuidad de negocio de los sistemas de información y comunicaciones críticos para el funcionamiento de la alianza. La creación de esta autoridad supuso un hito importante en el proceso de construcción de la ciberseguridad en la OTAN; ante una emergencia cibernética ésta es la autoridad a la que se debe acudir dentro de la OTAN. Esta autoridad coordina a través del Consejo de Gestión de Ciberdefensa – CDMB [8], del que forman parte los líderes de los comités político, militar, operacional y técnico de la OTAN con responsabilidades en ciberdefensa. Este consejo constituye el principal órgano de consulta de la OTAN en ciberdefensa y aconseja a los estados miembros. La autoridad opera bajo la División de Desafíos Emergentes de Seguridad[9]. La misión de esta autoridad es revisar y coordinar las capacidades.

Asistencia a las naciones

Antes de los ciberataques de Estonia de 2007, los esfuerzos en ciberdefensa de la OTAN se concentraban principalmente en la protección de los sistemas de comunicación propios y los que eran operados por la Alianza. Tras estos ataques, que se dirigieron contra servicios públicos y se realizaron a través de Internet, el objetivo de la OTAN se ha ampliado hacia la ciberseguridad de las naciones aliadas. Para ello la OTAN ha desarrollado mecanismos para asistir a los aliados que solicitan su apoyo en la protección de sus sistemas de comunicación, a través de Equipos de Respuesta Rápida[10]. No obstante, las naciones aliadas tienen la responsabilidad de la seguridad de sus sistemas de comunicación.

Investigación y Formación

El Centro de Excelencia OTAN de Ciberdefensa Cooperativa (Cooperative Cyber Defence Centre of Excellence -CCDCOE) en Tallinn, Estonia fue acreditado en 2008. Este centro se

[7] NATO Cyber Defence Management Authority-CDMA
[8] NATO Cyber Defence Management Board – CDMB
[9] Emerging Security Challenges Division in NATO HQ. Esta División comenzó a trabajar en agosto de 2010 y se centra sobre todo en terrorismo, proliferación de armas de destrucción masiva, ciberdefensa y seguridad energética.
[10] Rapid Reinforcement Teams -RRT

encarga de la investigación y formación en ciberguerra con personal experto de los diez países que lo patrocinan[11] (Estonia como país anfitrión, Alemania, Eslovaquia, España, EEUU, Hungría, Italia, Letonia, Lituania y Turquía). Su misión es mejorar la capacidad y cooperación de la OTAN y sus estados miembros en Ciberdefensa mediante el desarrollo de programas y proyectos de I+D+i, formación, análisis de casos reales y consulta.

Cooperación con los socios

La OTAN también desarrolla una cooperación práctica en ciberdefensa según las guías del Consejo para Cooperación en Ciberdefensa con los socios y organizaciones internacionales (aprobado en agosto de 2008), y del Marco de Cooperación en Ciberdefensa entre OTAN y los países socios (aprobado en abril de 2009).

La autoridad de gestión de ciberdefensa-CDMA apoyada, cuando es necesario, por el Comité de Planificación de Comunicación Civil, los Centros de Excelencia de Ciberdefensa de Tallinn y de Defensa contra el Terrorismo de Ankara, así como el Programa de Ciencia por la Paz y la Seguridad, ha organizado charlas de expertos, investigaciones, seminarios de formación, e intercambios de información entre los socios y organizaciones internacionales interesados (la Unión Europea y la OSCE[12]).

Los principales comités de decisión y de consejo

La OTAN articula sus decisiones a través de los siguientes organismos internos:

- El Consejo del Atlántico Norte – el comité político de decisión a más alto nivel – tiene el control total sobre las políticas y actividades relativas a ciberdefensa.
- El Comité de Planeamiento y Política de Defensa – DPPC[13], que sustituyó al Grupo de Trabajo Ejecutivo[14] en junio de 2010, ha desarrollado las propuestas a nivel político (es decir, preparación de una política de ciberdefensa y decisión OTAN sobre la creación de la Autoridad de Gestión de Ciberdefensa) para la aprobación por el Consejo.
- El Comité de Consulta, Mando y Control[15] - NC3 constituye el organismo principal de consulta de los aspectos técnicos y de implementación sobre ciberdefensa.
- Las Autoridades Militares [16] - NMA y la Agencia de Consulta, Mando y Control - NC3A[17] tienen la responsabilidad de identificar los requisitos operacionales y la adquisición e implementación de las capacidades de ciberdefensa.

[11] Véase www.ccdcoe.nato.int
[12] Organization for Security and Co-operation in Europe
[13] Defence Policy and Planning Committee
[14] Executive Working Group
[15] NATO Consultation, Control and Command (NC3)
[16] NATO Military Authorities (NMA)
[17] NATO's Consultation, Control and Command Agency (NC3A)

- La Agencia de los Servicios de Información y Comunicación- NCSA [18], a través de su centro técnico NCIRC[19], es responsable de la provisión de los servicios de ciberseguridad técnicos y operacionales. NCIRC desarrolla el papel clave de respuesta antes ciberagresiones a la OTAN. Proporciona medidas para gestionar e informar de los incidentes relacionados con los sistemas, gestión de la seguridad y usuarios. También se centra en la gestión de incidentes de manera centralizada y coordinada, evitando duplicidad de esfuerzos.

4. CONCLUSIÓN

Los ataques cibernéticos se han convertido en una fuente de amenazas en el mundo globalizado en que vivimos. Así lo contemplan ya algunos países de nuestro entorno y diversas organizaciones internacionales, algunos de los cuales ya han elaborado estrategias de ciberseguridad o ciberdefensa. La OTAN ha sido consciente de este riesgo emergente y como tal lo ha tratado en la agenda de sus cumbres, empezando por la Cumbre de Riga de 2006. Tras haber elaborado un concepto de ciberdefensa y una política de ciberdefensa, y haber establecido una estructura de gestión dentro de la estructura global de la OTAN, la Alianza continúa avanzando en el ámbito de ciberdefensa tras la Cumbre de Lisboa. Esta cumbre marcó una hoja de ruta cuyo primer hito se cumplió en la reunión de Bruselas del pasado 10 de marzo, con la definición de un nuevo concepto de ciberdefensa. El segundo hito consistente en la elaboración de una nueva política de ciberdefensa y el desarrollo de un plan de acción está planificado para la próxima reunión de los ministros de Defensa del próximo junio.

Madrid, 17 de marzo de 2011
María José Caro Bejarano
Analista principal del IEEE

[18] NATO Communication and Information Services Agency (NCSA)
[19] NATO Computer Incidents Response Capability Technical Centre (NCIRC)