ieee.es
Instituto Español de Estudios Estratégicos

Documento
Informativo

37/2011 5 octubre de 2011

Mª José Caro Bejarano

LA NUEVA POLÍTICA DE
CIBERDEFENSA DE LA OTAN

LA NUEVA POLÍTICA DE CIBERDEFENSA DE LA OTAN

RESUMEN:

Los ministros de defensa de la OTAN aprobaron el 8 de junio la nueva política de ciberdefensa, uno de los compromisos de la cumbre de Lisboa de noviembre de 2010. El Concepto de Ciberdefensa se revisó y aprobó en la reunión de los ministros en marzo de este año. Esta política de ciberdefensa revisada se acompaña de un Plan de Acción, un documento detallado con las tareas y actividades específicas para las propias estructuras de la OTAN y las fuerzas defensivas de sus aliados.

ABSTRACT:

On June 8th *the NATO* Defence Ministers approved the revised NATO Policy on Cyber Defence, one of the commitments from the 2010 Lisbon Summit. The revised Concept on Cyber Defence was first drafted for Defence Ministers in March 2011. This revised cyber defence policy is coupled with an Action Plan, a detailed document with specific tasks and activities for NATO's own structures and Allies' defence forces.

Palabras clave:

OTAN, ciberdefensa, ciberataques, ciberdefensa.

Keywords:

NATO, cyber defence, cyber attacks, cyber defence.

ANTECEDENTES

El pasado 10 de marzo los ministros de Defensa de la OTAN aprobaron el *Nuevo Concepto de Ciberdefensa* de la Alianza[1]. Continuando con la agenda de la OTAN, en la pasada reunión de junio aprobaron una revisión de la Política de Ciberdefensa y un Plan de Acción de Ciberdefensa, que representa el documento detallado con tareas y actividades específicas para las propias estructuras de la OTAN y las fuerzas defensivas de sus aliados.

El entorno de seguridad de esta década ha cambiado notablemente. Las sociedades y economías modernas están interconectadas por redes, cables y direcciones IP de ordenadores y otros dispositivos móviles. Al aumentar la dependencia de los sistemas CIS (Communitations and Information Systems), la Alianza debe adaptarse y mejorar sus defensas para enfrentarse a estos desafíos emergentes. Por este motivo, la política revisada de Ciberdefensa de la OTAN establece una clara visión de los planes para impulsar estos esfuerzos.

El Nuevo Concepto Estratégico de 2010[2] destacaba la necesidad de "desarrollar nuestra capacidad de prevenir, detectar, defenderse y recuperarse de ciberataques…". Las amenazas están evolucionando muy rápido en frecuencia y sofisticación. Las amenazas que provienen del ciberespacio – Estados, hacktivistas u organizaciones criminales, entre muchos otros – plantean un desafío considerable a la Alianza y debe tratarse con un asunto urgente.

Como visión general la Política se plantea desarrollar las tareas principales de la Alianza: la defensa colectiva y la gestión de crisis; y garantizar la integridad y disponibilidad de los sistemas de información. Por ello el principal foco es la protección de sus sistemas CIS. Además, para defender estos sistemas y redes, la OTAN mejorará sus capacidades ante el amplio abanico de ciberamenazas a que se enfrenta.

Como objetivos, la OTAN implementará un enfoque coordinado de ciberdefensa para abarcar aspectos de planificación y desarrollo de capacidades junto con mecanismos de respuesta en caso de ciberataque. Para ello la Alianza incorporará e integrará las medidas de ciberdefensa en las misiones.

---

[1] Documento Informativo del IEEE 09/2011, Nuevo Concepto de Ciberdefensa de la OTAN, (marzo de 2011).
[2] Nuevo Concepto Estratégico de la OTAN, véase en http://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf.

Los esfuerzos en ciberdefensa de la OTAN están basados en los principios generales de prevención, resiliencia y no-duplicación. Los dos primeros son particularmente importantes dado que ciertas amenazas persisten a pesar de todos los esfuerzos de protección y defensa. La prevención ante nuevos ataques se alcanzará incrementado el nivel de preparación y mitigando el riesgo limitando las interrupciones y sus consecuencias. La resiliencia es clave ya que facilita la rápida recuperación tras un ataque.

Como se establece en el Nuevo Concepto Estratégico, la OTAN defenderá su territorio y a su población contra toda amenaza, incluyendo los desafíos a la seguridad emergentes como la ciberdefensa. Esta política de ciberdefensa reitera que la cualquier respuesta de defensa colectiva está sujeta a las decisiones del Consejo. La OTAN mantiene una ambigüedad estratégica y flexibilidad para responder a diferentes tipos de crisis que incluyan un componente cibernético. También integrará el aspecto cibernético en los procedimientos de gestión de crisis, que guiarán la respuesta OTAN dentro del contexto de una crisis o conflicto largo.

La OTAN proporcionará asistencia coordinada si uno o varios aliados son víctimas de un ciberataque. Para facilitar esto, se mejorarán los mecanismos de consulta, alerta temprana, conciencia de la situación y compartirá información entre los aliados. Para la respuesta a incidentes dentro de la estructura de información de la OTAN la capacidad de respuesta ante incidentes NCIRC (NATO Computer Incident Response Capability) vigila diariamente y aplica las medidas apropiadas.

Para aplicar esta gobernanza en ciberdefensa el Consejo se apoya en el Comité de Planificación y Política de Defensa, éste en el Comité de Gestión de Ciberdefensa y éste a su vez, en el NCIRC anteriormente mencionado.

Como pasos prácticos:

- La OTAN desarrollará unos requisitos mínimos para los sistemas nacionales de información que son críticos para desarrollar las tareas principales.
- La OTAN asistirá a los aliados para alcanzar un nivel mínimo de ciberdefensa para reducir las vulnerabilidades de las infraestructuras críticas.
- Los aliados pueden ofrecer su ayuda a otro aliado o a la Alianza en caso de un ciberataque.
- La ciberdefensa se integrará completamente dentro del proceso de planeamiento de la defensa y en las estructuras OTAN para desarrollar las tareas principales de defensa colectiva y gestión de crisis.

- Las autoridades militares OTAN valorarán el apoyo de la ciberdefensa a las tareas principales de la OTAN, el planeamiento de las misiones militares y el despliegue de las misiones.
- También se definirán requisitos de ciberdefensa para las naciones que contribuyan con tropas y no pertenecientes a la OTAN.
- Tanto la OTAN como los aliados cuentan con el conocimiento y apoyo del Centro de Excelencia OTAN de Ciberdefensa Cooperativa[3] en Tallinn, Estonia.
- Involucrar a socios, organizaciones internacionales, sector privado y ámbito académico.

La nueva capacidad de la OTAN en ciberdefensa es una de los once proyectos prioritarios acordados en la cumbre de Lisboa del pasado noviembre. Con un coste de 28 millones de euros representa casi el triple de la inversión de la alianza en la protección de sus redes.

Mª José Caro Bejarano
Analista Principal del IEEE

[3] Cooperative Cyber Defence Centre of Excellence, CCDCOE.