ieee.es
Instituto Español de Estudios Estratégicos

Documento
Informativo

13/2014 15 octubre de 2014

David Ramírez Morán

LA CIBERDEFENSA EN LA CUMBRE DE GALES DE LA OTAN

LA CIBERDEFENSA EN LA CUMBRE DE GALES DE LA OTAN

Resumen:

En la Cumbre de Gales de la OTAN se han alcanzado acuerdos significativos en el campo de la ciberdefensa de gran interés para los países que conforman la Alianza. Estos acuerdos tratan diversos aspectos que incluyen las políticas y las actividades que deberá desarrollar la Alianza para alcanzar los objetivos de ciberdefensa necesarios para la protección de los Estados.

Abstract:

In the Wales NATO Summit significant agreements on cyberdefence have been reached, of great interest for the countries conforming the Alliace. These agreements deal with several aspects including the policies and activities that the Alliance should develop to reach the cyberdefence targets required for the protection of the States.

Palabras clave:

Ciberdefensa, OTAN, Cumbre de Gales, legislación, campos de pruebas, industria.

Keywords:

Cyberdefence, NATO, Wales Summit, legislation, test ranges, industry.

INTRODUCCIÓN

La Cumbre de la OTAN celebrada en Cardiff (Gales) los días 4 y 5 de septiembre de 2014 ha recibido una gran atención debido a la concurrencia del conflicto en curso en Ucrania y las acciones que está llevando a cabo el Estado Islámico en Oriente Próximo. Además de estos temas, la agenda de la cumbre incluía otros temas que también conllevan una considerable importancia para la Alianza entre los que figuraban cuestiones relativas a la ciberdefensa.

La ciberdefensa lleva ya bastantes años formando parte de los temas de interés de la alianza y cuenta actualmente con una política de ciberdefensa específica cuya última modificación ha sido refrendada en esta cumbre. Los acuerdos alcanzados en la cumbre incluyen temas legislativos así como líneas de acción que deberán desarrollar los países para alcanzar una capacidad de defensa efectiva.

ANTECEDENTES

La ciberdefensa forma parte del Concepto Estratégico de la Alianza desde la Cumbre de Lisboa de 2010, después de que en enero de 2008 se desarrollara la primera Política de Ciberdefensa a raíz de los eventos que se habían producido el año anterior con el ciberataque a Estonia. En la cumbre de Lisboa se encargó al NAC la elaboración de una nueva Política de Ciberdefensa así como la determinación de las líneas de acción necesarias para su implementación.

En 2011, los Ministros de Defensa aprobaron la segunda Política de Ciberdefensa de la OTAN en la que se implantaba una visión de esfuerzos colaborativos en el contexto de las rápidas evoluciones de la tecnología y de las amenazas y se fijaban las líneas de acción para ejecutarla.

En abril de 2012, comenzó la integración de la ciberdefensa en el Proceso de Planeamiento de la Defensa de OTAN, lo que dio lugar a que se identificaran y priorizaran los requerimientos relevantes para la ciberdefensa. Más tarde, en la cumbre de Chicago celebrada en mayo de 2012 se reafirmó el compromiso de mejora de las ciberdefensas de la alianza reuniendo todas las redes de OTAN bajo una protección centralizada e implementando mejoras de la NCIRC[1]. También ese año, en julio, se creó la NCIA[2], en la que se integraban las seis agencias existentes relacionadas con las tecnologías de la información y telecomunicaciones.

Los Ministros de Defensa aliados encargaron a OTAN el desarrollo de una nueva y mejorada política de ciberdefensa que abordara la defensa colectiva, la asistencia a los Aliados, la delineación de la gobernanza, las consideraciones legales y la relación con la industria. Esta

[1] NCIRC: NATO Computer Incident Response Capability
[2] NCIA: NATO Communications and Information Agency

nueva política, refrendada por los Ministros de Defensa de OTAN en junio de 2014 constituye la principal referencia en lo que respecta al tratamiento de la ciberseguridad en el seno de la OTAN.

Los acuerdos alcanzados durante la cumbre de Gales se han recogido en los párrafos 72 y 73 de la Declaración de la Cumbre de Gales[3] emitida por los jefes de Estado y Gobierno participantes.

LA CIBERDEFENSA EN LA ALIANZA

Todos los factores políticos que se han acordado en la cumbre en relación con la ciberdefensa se han recogido en el párrafo 72 de la Declaración.

En primer lugar se detalla la visión de la Alianza por la que considera que los ataques cibernéticos van a continuar produciéndose y cada vez serán más comunes, sofisticados y contarán un mayor potencial de producir daños.

La ciberdefensa pasa a ser una de las actividades principales de la Alianza como viene recogido en la Política de Ciberdefensa Mejorada. Se reafirman los principios de indivisibilidad de la seguridad de los Aliados, de prevención, de detección, de resiliencia, de recuperación y de defensa.
Se recuerda también que la responsabilidad fundamental de ciberdefensa de la OTAN es la de proteger sus propias redes, y que la asistencia a los Aliados debería abordarse de acuerdo al principio de solidaridad, haciendo énfasis en la responsabilidad de los Aliados de desarrollar las capacidades relevantes para la protección de las redes nacionales.

En línea con lo recogido en el Manual de Tallín[4], la política reconoce la aplicabilidad al ciberespacio de la legislación internacional, incluyendo la legislación internacional humanitaria y la Carta de las Naciones Unidas.

Se reconoce que los ciberataques pueden alcanzar un nivel que amenace la prosperidad, securidad y estabilidad Euro-Atlántica. El daño que pueden suponer para las sociedades modernas se equipara al de un ataque convencional. De esta forma se afirma que la ciberdefensa constituye una tarea principal de la defensa colectiva de la OTAN.

En relación a la decisión sobre cuándo un ciberataque motivaría la invocación del Artículo 5 del Tratado de Washington, se tomará bajo un criterio de caso por caso por el Consejo del Atlántico Norte.

[3] Wales Summit Declaration http://www.nato.int/cps/en/natohq/official_texts_112964.htm (Consultado 15/10/2014)
[4] Tallinn Manual on the International Law Applicable to Cyber Warfare http://www.ccdcoe.org/tallinn-manual.html (consultado 15/10/2014)

EL COMPROMISO DE LOS PAÍSES

Las líneas de acción necesarias para la puesta en marcha de las políticas requiere el compromiso de los países para participar de forma activa en estas actividades. Estos compromisos se han recogido en el párrafo 73 de la Declaración.

Algunos países han destacado recientemente la desigualdad velocidad con la que se están desarrollando las capacidades de ciberdefensa de los diferentes Estados. En esta línea, los Aliados han acordado seguir desarrollando sus capacidades nacionales de ciberdefensa y mejorar la ciberseguridad de las redes nacionales de las que depende la OTAN para el desarrollo de sus tareas principales. De este modo se persigue el objetivo de protección total y de resiliencia de la Alianza.

Se destaca nuevamente el importante papel que juega la estrecha cooperación bilateral y multinacional para mejorar las capacidades de ciberdefensa. De esta forma se refleja el compromiso de las naciones en seguir aportando información y participando en las actividades que permiten el avance de los desarrollos, tanto técnicos como procedimentales, en este campo.

En respuesta directa a las directrices políticas, los Estados seguirán integrando la ciberdefensa en las operaciones de la OTAN y en el planeamiento operacional y de contingencia. También potenciarán la compartición de la información y de la conciencia situacional entre los Aliados.

Para abordar los riesgos y amenazas cibernéticos se destaca el papel fundamental que juegan las colaboraciones entre los diferentes actores. Así, los Aliados participarán activamente en eventos cibernéticos con otros países relevantes bajo un criterio de caso a caso, así como con otras organizaciones internacionales como al Unión Europea. En respuesta a la necesidad de colaboración con las empresas recogida en las directrices, se intensificará la cooperación mediante el NATO Industry Cyber Partnership, mecanismo que contribuye a la colaboración entre las organizaciones y las empresas del sector.

Los Estados también mejorarán las actividades relativas a la formación, entrenamiento y a los ejercicios sobre ciberdefensa de la OTAN.

Las naciones han acordado el desarrollo de una capacidad de campo de pruebas cibernético que, inicialmente, se creará alrededor de la instalación existente en Estonia. Para el desarrollo de esta capacidad se tendrán en cuenta las capacidades y requerimientos de la Escuela CIS OTAN y de otros organismos de educación y entrenamiento de la OTAN.

CONSIDERACIONES ADICIONALES

La política basa las acciones de defensa colectiva en la colaboración internacional haciendo recaer el peso principalmente sobre las herramientas desarrolladas por los distintos estados

para asegurar su ciberdefensa. De esta forma, se omite la discusión relativa a las ciberarmas, que permiten realizar operaciones ofensivas, dejando todas las actividades de la Alianza en caso de aplicación del Artículo 5 en la colaboración entre los países miembros, que aportarían información y colaboración a las autoridades locales.

La falta de estandarización sobre las herramientas defensivas, de explotación y ofensivas que existe en la actualidad es achacable no sólo a la rápida evolución tecnológica que se está produciendo en el sector, sino también al interés, cuya licitud es cuestionable, que tienen los países en mantener en secreto al disponibilidad de herramientas o armas de ciberdefensa. Ante el apoyo que se refleja en el documento al entorno de la industria de defensa, esta falta de estandarización y la práctica inexistencia de un mercado, supone un revés para el sector de la ciberseguridad. Con el escenario actual, las soluciones tienen que venir de manos de empresas locales, lo que constituye un serio handicap para la Alianza al requerir la multiplicación de los esfuerzos financieros e industriales necesarios para alcanzar un grado de protección dado. Esta situación es consecuencia de la naturaleza del ciberespacio, donde la incertidumbre sobre la naturaleza y origen de la amenaza da lugar a que se guarde con celo toda información que pueda suponer una ventaja ante un ataque.

Otro punto para el que se esperaba una mayor concreción como resultado de la cumbre es el de la gradación de los incidentes cibernéticos. Para invocar el Artículo 5 es necesario que uno de los países miembros esté siendo atacado. Sin embargo, no existe legislación a partir de la cual determinar cuándo una actividad cibernética constituye un ataque a la soberanía de un país.

La velocidad con la que opera la amenaza cibernética requiere respuestas rápidas, si no inmediatas, para lo que sería deseable disponer de unos criterios claros y específicos sobre cuándo poner en marcha una operación de defensa colectiva. Esto permitiría reducir drásticamente los tiempos de reacción adaptándolos de forma más acorde a las temporizaciones que caracterizan un ataque cibernético. Sin embargo, la solución adoptada no define los criterios y, además de someter la decisión a un análisis caso por caso, requiere la decisión del Consejo del Atlántico Norte, lo que puede dar lugar a plazos de decisión demasiado extensos. A estos efectos, la determinación de un comité específico asociado a un régimen de urgencia permitiría agilizar la respuesta ante una situación de ataque.

Resulta destacable la reducida diferenciación que se produce en el tratamiento de las amenazas cibernéticas entre el mundo militar asociado a la OTAN y el mundo civil, reflejado en las numerosas correspondencias existentes entre la política de ciberdefensa de OTAN y las estrategias de seguridad desarrolladas por la Unión Europea, España y otras naciones. En ambos casos, la colaboración tanto institucional como con la industria, la formación, el entrenamiento y la realización de ejercicios conjuntos son las herramientas que se ponen sobre la mesa para alcanzar los objetivos de ciberseguridad.

CONCLUSIONES

La situación geopolítica actual, donde los conflictos de Ucrania y la rápida expansión del Estado Islámico han acaparado gran parte de la atención, ha eclipsado el avance que se está produciendo en el mundo de la ciberdefensa en el marco de la OTAN. No cabe duda de que se ha producido un avance significativo gracias a la nueva consideración que se ha dado a los ataques cibernéticos, que pasan a constituir motivo suficiente para la invocación del Artículo 5 de defensa colectiva del Tratado de Washington.

En el marco de las actividades, se sigue fomentando la colaboración internacional tanto en tiempo de paz como en un eventual escenario de batalla. Sin embargo, la labor que se encomienda a la OTAN, aunque no se excluyen tácitamente otras actividades, se reduce a la colaboración con los otros países para, con las herramientas desarrolladas por estos, abordar la labor de defensa contra el ciberataque. En ningún momento se considera la posibilidad de intercambiar o implantar un mercado de herramientas estandarizadas que permita dotarse de capacidades de ciberdefensa.

Al igual que la Estrategia de Ciberseguridad de la Unión Europea, la nueva política de la alianza basa las acciones a realizar en la colaboración entre Estados, la realización de ejercicios y la necesidad de que todos los actores involucrados adopten una postura activa en la gestión de la ciberseguridad y la ciberdefensa.

La Política de Ciber Defensa Mejorada recuerda que la principal responsabilidad de OTAN es defender sus propias redes y que la asistencia a los aliados debería abordarse de acuerdo a los principios de solidaridad, enfatizando la responsabilidad de los aliados de desarrollar las capacidades relevantes para la protección de las redes nacionales.

No cabe duda de que el quinto espacio de confrontación, el ciberespacio, al igual que los cuatro previamente existentes, presenta una problemática que requiere un tratamiento particularizado. Las soluciones que resultan de aplicación en los otros espacios no se adaptan a la situación existente y será necesario desarrollar un nuevo marco que proporcione las condiciones necesarias para alcanzar un grado de protección comparable. Esta singularidad que se destaca en el campo de la ciberdefensa se enmarca a su vez en el problema aun mayor asociado a la ciberseguridad tanto en el mundo civil como en el mundo militar.

David Ramírez Morán
Analista del IEEE