# Ciberdefensa, una necesidad operativa

**Federico Yaniz Velasco**
***General (retirado)***
***del Ejército del Aire y del Espacio***
***Exdirector adjunto del EMI***

*El nuevo centro militar OTAN de operaciones cibernéticas estará operativo este año 2023*

Los ataques cibernéticos se caracterizan por su complejidad y su capacidad de aniquilamiento de elementos esenciales para el funcionamiento de centros neurálgicos de la defensa. El espacio cibernético se ve constantemente sometido a desafíos de diferente carácter y gravedad. Las naciones aliadas y la OTAN en su conjunto responden a esos retos fortaleciendo su capacidad de la Alianza para detectar, prevenir y responder a actividades cibernéticas malévolas. Los aliados descansan en ciberdefensas fuertes y resilientes para poder cumplir tres tareas fundamentales: disuasión y defensa, prevención y gestión de crisis, así como seguridad cooperativa. Para la OTAN desarrollar y mantener una defensa cibernética adecuada ha sido y es una necesidad operativa.

Los sistemas de información y en general las comunicaciones de la OTAN siempre han estado bien protegidas. Sin embargo, hasta el año 2002 la defensa cibernética no se incluyó en su agenda. En efecto, fue en la cumbre de Praga cuando los líderes aliados consideraron por primera vez la ciberdefensa entre los asuntos a tratar. Cuatro años después los líderes aliados destacaron en la cumbre de Riga la necesidad de proporcionar una protección adicional a los sistemas de información.

Tras los ataques cibernéticos en 2007 contra instituciones públicas y privadas de Estonia, los ministros de Defensa aliados acordaron que era necesario trabajar urgentemente en todo lo relacionado con esa amenaza. Como resultado, la OTAN aprobó su primera política de ciberdefensa en enero de 2008. Ese mismo año estalló el conflicto entre Rusia y Georgia. En esa ocasión se pudo comprobar que los ataques cibernéticos son relevante en conflictos y guerras. Como consecuencia, en el Concepto Estratégico adoptado en la cumbre de 2010 se reconoció por primera vez que los ataques cibernéticos podrían alcanzar el umbral de amenaza para la prosperidad, la seguridad y la estabilidad nacionales y euroatlánticas.

En junio de 2011, los ministros de Defensa aliados aprobaron la revisión de la doctrina OTAN sobre ciberdefensa. En ella se estableció una nueva aproximación a la ciberdefensa teniendo en cuenta la evolución de las amenazas y los avances tecnológicos. En abril de 2012 la ciberdefensa se incluyó en el proceso de planeamiento de Defensa. En la cumbre celebrada en Chicago los días 20 y 21 de mayo, los entonces 27 líderes aliados reafirmaron su compromiso de mejorar la ciberdefensa de la Alianza. Para ello se pusieron todas las redes de la OTAN bajo protección centralizada y se implementaron una serie de mejoras en la capacidad de ciberdefensa. Además en el mes de julio, en el marco de la reforma de las agencias aliadas, se creó la Agencia OTAN de Comunicación e Información.

El Consejo del Atlántico Norte acordó en abril de 2014 adoptar el nombre de Cyber Defence Committee para el órgano superior asesor en asuntos de ciberdefensa. El 5 de septiembre, los lideres aliados adoptaron

en la cumbre celebrada en Newport (Gales) la nueva doctrina aliada de ciberdefensa y se reconoció también que un ataque cibernético podría motivar la invocación del artículo 5 del tratado de Washington. Los aliados también reconocieron que el derecho internacional es aplicable en el ciberespacio. Poco después, en septiembre de 2014, la OTAN lanzó una iniciativa para favorecer la cooperación con el sector privado y enfrentarse juntos a las amenazas y desafíos cibernéticos. En ese contexto se presentó en Mons (Bélgica) la Asociación OTAN de la industria cibernética (NICP).

En el mes de febrero de 2016 la OTAN y la UE concluyeron un acuerdo técnico sobre ciberdefensa para contribuir a prevenir y responder eficazmente a los ciberataques. Este acuerdo técnico proporciona el marco adecuado para intercambio de información entre los equipos de respuesta a emergencias. Por otra parte, en agosto se celebró la cumbre de Varsovia en la que se reafirmaron el carácter defensivo de la OTAN y reconocieron el ciberespacio como un dominio operativo en el que la OTAN tiene que defenderse. La Alianza también acogió con complacencia los esfuerzos realizados en otros foros internacionales para desarrollar normas de comportamiento responsable de los estados y las medidas de fomento de la confianza para alcanzar un ciberespacio más transparente y estable. En la cumbre de Varsovia, los aliados alcanzaron también, como cuestión prioritaria, un compromiso en ciberdefensa para mejorar las ciberdefensas de sus redes e infraestructuras nacionales. Todos los aliados se comprometieron a mejorar su resiliencia y su capacidad para responder rápida y eficazmente a las amenazas cibernéticas, incluso como parte de campañas de guerra híbrida. En diciembre la OTAN y la UE acordaron más de 40 medidas para trabajar juntas, incluida la lucha contra las amenazas híbridas, la ciberdefensa y la mejora de su vecindad común. En cuanto a la ciberdefensa, la OTAN y la UE acordaron reforzar su participación en ejercicios y fomentar la investigación, la formación y el intercambio de información.

Los ministros de Defensa aprobaron en febrero de 2017 un plan de acción de ciberdefensa actualizado, así como una hoja de ruta para implementar el ciberespacio como un dominio operativo. Esto aumentó la capacidad de los aliados para trabajar juntos, desarrollar capacidades y compartir información. En ese mismo mes, la OTAN y Finlandia (que en ese momento era un país socio y que pasó a ser el miembro 31 el 4 de abril de 2023) intensificaron su compromiso de colaboración con la firma de un acuerdo marco sobre ciberdefensa. El acuerdo hacía posible que la OTAN y Finlandia protegiesen sus redes y mejorasen su resiliencia. En diciembre, los ministros de la OTAN y la UE acordaron intensificar la cooperación entre las dos organizaciones en una serie de áreas, incluida la ciberseguridad y la ciberdefensa. Esa cooperación incluye el análisis de las amenazas cibernéticas y la colaboración entre equipos de respuesta a incidentes, así como el intercambio de buenas prácticas incluyendo aspectos cibernéticos y sus implicaciones en la gestión de crisis.

En la Cumbre de Bruselas de julio de 2018, los líderes aliados acordaron establecer un nuevo centro de operaciones del ciberespacio como parte de la estructura de mando de la OTAN. El centro coordina las actividades operativas aliadas en y a través del ciberespacio. Los aliados también decidieron que la OTAN podría aprovechar las capacidades cibernéticas nacionales para sus operaciones y misiones.

Los ministros de Defensa aliados aprobaron en febrero de 2019 una guía que señala unas herramientas para fortalecer la capacidad aliada de responder a actividades cibernéticas malévolas. La OTAN necesita utilizar todas las herramientas a su disposición, incluidas las políticas, diplomáticas y militares, para hacer frente a las amenazas cibernéticas. Las opciones de respuesta descritas en la mencionada guía ayudan a los aliados a mejorar su conocimiento de lo que está sucediendo en el ciberespacio, a aumentar su resiliencia y a trabajar junto con los socios para disuadir, defender y contrarrestar todo el espectro de amenazas cibernéticas.

En la cumbre celebrada en Bruselas el 14 de junio de 2021 los líderes aliados respaldaron una nueva política integral de ciberdefensa para apoyar las tres tareas principales de la OTAN, así como su postura general de disuasión y defensa. Los aliados reconocieron que la acumulación de ciertas actividades cibernéticas malévolas podría considerarse, en determinadas circunstancias, un ataque armado. En septiembre de 2021, el CAN nombró a su primer Director de Información (CIO) para facilitar la integración, alineación y cohesión de los sistemas de Tecnología de la Información y Comunicaciones (TIC) en toda la OTAN.

En la cumbre celebrada en Vilna el 11 de julio de 2023, los aliados endosaron un nuevo concepto para mejorar la contribución de la ciberdefensa a la disuasión general y a la postura defensiva de la OTAN. En Vilna, los aliados endosaron una nueva versión del compromiso de ciberdefensa y se comprometieron a fortalecer prioritariamente las ciberdefensas nacionales. Por otra parte, reconociendo la necesidad de recibir asistencia rápidamente, la OTAN activó la capacidad virtual de apoyo a incidentes cibernéticos (VCISC) para apoyar los esfuerzos nacionales de respuesta a actividades cibernéticas malévolas importantes.