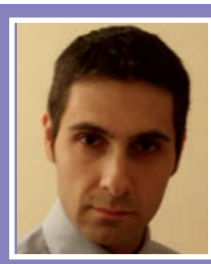
Construyendo la Ciberdefensa Aliada

El pasado mes de julio se celebró en Varsovia la última Cumbre de Jefes de Estado o de Gobierno de la Alianza Atlántica. La agenda del encuentro cubrió numerosos aspectos de actualidad[1], el grueso de ellos relacionados con la Federación rusa (la creciente asertividad en su área de influencia y el empleo de estrategias híbridas, las relaciones entre la OTAN y Ucrania o el refuerzo de la presencia militar en los países bálticos), el compromiso suscrito en la Cumbre de Gales (2014) de incrementar el gasto en defensa de los veintiocho o la consolidación de la ciberdefensa aliada tres lustros después de que la OTAN tomara conciencia del valor estratégico del ciberespacio. Precisamente, este artículo pretende repasar la evolución de la ciberdefensa aliada desde sus inicios hasta la actualidad.

La toma de conciencia del potencial que posee el ciberespacio en las actividades de la Alianza Atlántica se produjo en 1999. Durante el transcurso de Operación Fuerza Aliada para forzar la retirada serbia de Kosovo y coincidiendo con el bombardeo de la embajada china en Belgrado, hacktivistas serbios, rusos y chinos llevaron a cabo varios ataques de Denegación de Servicio (DoS) y *defacements* sobre los sitios web de la OTAN[2]. Aunque irrelevantes más allá de su impacto informativo[3], estos incidentes mediaron para que la Alianza estimara necesario incrementar la seguridad de sus redes informáticas, instar a que sus miembros mejoraran sus capacidades tecnológicas y cooperar con otros actores –en particular la Unión Europea y el sector industrial– para salvaguardar sus redes de información y comunicaciones.

Sin embargo, fue necesario esperar hasta la Cumbre de Praga (2002) para que la OTAN reconociera la importancia del ciberespacio en la guerra moderna. Condicionada por los sucesos del 11 de Septiembre de 2001, la euforia tecnocéntrica estadounidense tras la invasión de Afganistán y el arranque de la transformación militar aliada, en la capital checa se lanzaron varias iniciativas que sentaron los pilares de la ciberdefensa aliada. No solo se avaló políticamente la conveniencia de incrementar la protección y resiliencia de los Sistemas de Información y Comunicaciones (CIS) de la organización y resolvió constituir la Capacidad de Respuesta a Incidentes Informáticos *(NATO Computer Incident Response Capability* – NCIRC) para prevenir, detectar y gestionar cualquier contingencia que pudiera afectar las redes informáticas aliadas; sino que el Compromiso de Capacidades de Praga[4] incluyó el denominado *NATO Cyberdefence Programme*, un paquete de medidas específicamente incardinadas a modernizar los sistemas C3I y mejorar la seguridad de las infraestructuras CIS nacionales. Mientras NCIRC logró la plena capacidad operativa en 2014, el Paquete de Capacidades de Praga –que reemplazaba la Iniciativa de Capacidades de Defensa de 1999– fue implementado de manera parcial, puesto que muchos socios europeos –reticentes a asumir sus compromisos y desconocedores del valor del ciberespacio para la seguridad nacional– solamente desarrollaron de manera limitada ciberdefensas pasivas.

Aunque la Guía de Política General (*Comprehensive Planning Guidance*) –aprobada por el Consejo del Atlántico Norte en 2005 y refrendada en la Cumbre de Riga de 2006 para llenar el vacío estratégico existente entre los Conceptos Estratégicos de Washington (1999) y Lisboa (2010)– reconocía el valor intrínseco del ciberespacio para la seguridad euroatlántica, no fue hasta los ciberataques contra Estonia de 2007 cuando la OTAN tomó conciencia de los efectos técnicos y las implicaciones políticas que podían tener este tipo de incidentes. La alarma estaba plenamente justificada: el país quedó paralizado durante varios días tras una campaña de ataques de Denegación de Servicio Distribuido (DDoS) realizados por hacktivistas rusos que, supues-



Guillem Colom Piella
Doctor en Seguridad Internacional

Clara Rodríguez Chirino
Graduada en Relaciones Internacionales y Traducción e Interpretación

tamente coordinados desde el Kremlin, penetraron en la administración pública y el sistema bancario del país hasta el punto que el primer ministro estonio consideró, aparentemente, invocar el Artículo 5 del Tratado de Washington[5]. Esta toma de conciencia medió para que la Alianza aprobara su primer *Concepto de Ciberdefensa* y articulara su primera *Política de Ciberdefensa*, avaladas por los jefes de estado o de gobierno de la OTAN en la Cumbre celebrada en Bucarest en abril de 2008. Precisamente, este encuentro que reconocía *"… el compromiso en mejorar los sistemas clave de información aliados contra ciberataques […] compartir las buenas prácticas y proporcionar la capacidad de asistir a los países aliados –bajo petición– para contrarrestar un ciberataque."*[6] sentó las bases de la denominada *Ciberdefensa 1.0*. Basada en los principios de **subsidiariedad** (para evitar en lo posible el *free-riding* en la generación de cibercapacidades), **no duplicación** (para evitar el división de esfuerzos) y **seguridad** (para garantizar la trasparencia y confianza mutuas). Ello medió para que la ciberdefensa empezara a tener su propio espacio en la agenda político-militar aliada hasta consolidarse en el Concepto Estratégico de 2010, presentado en la Cumbre de Lisboa.

Aunque la gestación del nuevo Concepto Estratégico estuvo plagado de contratiempos y controversias entre los aliados[7], éstos –quizás tras evidenciar durante la guerra entre Rusia y Georgia de verano de 2008 que los ciberataques podían apoyar la conducción de operaciones convencionales– asumieron la importancia estratégica del ciberespacio para la seguridad euroatlántica. Asumiendo que el entorno cibernético estaría presente en los conflictos futuros, la OTAN se dispuso a generar las capacidades necesarias para detectar, evaluar, pre-

venir, defenderse, recuperarse de ciberataques enemigos, sentando así las bases de la *Ciberdefensa 2.0*: se instó al Consejo del Atlántico Norte a desarrollar una nueva *Política de Ciberdefensa* que sustituyera a la de 2008, se elevó la categoría de los ciberataques hasta el punto de poder ser constitutivos de la activación el Artículo 5 del Tratado de Washington; se avaló el valor de la ciberdefensa para la consecución de la defensa colectiva, la gestión de crisis y la seguridad cooperativa (las tres labores básicas de la OTAN identificadas en el Concepto Estratégico de 2010) y se desarrolló el *Paquete de Capacidades de Lisboa* para subsanar las carencias más importantes. Además, con el fin de asistir a los miembros en materia de protección y respuesta, se establecieron dos Equipos de Reacción Rápida (*Rapid Reaction Teams* – RRT) para hacer frente a crisis cibernéticas que afecten a la Alianza, así como de apoyar subsidiariamente a las redes nacionales en caso de ciberataque. Aunque proporcionan una limitada asistencia técnica (ayudando a proteger o restablecer los sistemas y coordinar la respuesta), los RRT tienen un fuerte valor político al afianzar el compromiso de la Alianza a la hora de apoyar sus propios sistemas y a los de los aliados.

La aprobación de la nueva *Política de Ciberdefensa* en 2011 no solo permitió que ésta pasara a formar parte del proceso de planeamiento de la defensa aliada para identificar, generar, priorizar y presupuestar las capacidades necesarias para lograr los objetivos de ciberdefensa de la organización, sino que ésta también se incluyó –durante la Cumbre de Chicago de 2012– en la *Smart Defence* que, basada en la priorización del gasto, la cooperación tecnológica y la especialización nacional, pretende establecer sinergias entre los veintiocho para generar las capacidades militares aliadas necesarias para los conflictos futuros en este marco de crisis económica. Ese mismo año, como fruto de la fusión de varias agencias de la Alianza, se creó la Agencia de Comunicaciones e Información de la OTAN (*NATO Communications and Information Agency* – NCIA) con el fin de armonizar e integrar los sistemas y capacidades C[4]ISR de la organización.

Aunque parecía que la OTAN se había tomado muy en serio la consolidación de su vertiente cibernética, en 2013 se produjo una llamada de atención a los aliados porque muchos parecían haber adoptado una postura de *free-riders* para aprovecharse de las cibercapacidades aliadas sin la necesidad de invertir en sus ciberdefensas nacionales[8]. En efecto, en la Reunión de Ministros de Defensa de octubre no solo se resolvió la necesidad de mejorar las capacidades cibernéticas nacionales, que deben ser compatibles con las de la OTAN y los demás aliados; sino que también recordó a los veintiocho que las capacidades de ciberdefensa aliadas cubren las necesidades operativas del Cuartel General, la Estructura de Mandos y sus organismos asociados, estando a disposición de los aliados solamente en caso de necesidad[9].

En 2014, se aprobó la tercera *Política de Ciberdefensa* que, avalada políticamente en la Cumbre de Gales, actualmente se halla en proceso de implementación. Durante este encuentro, y en línea con los planteamientos del Concepto Estratégico 2010, los jefes de estado o de gobierno ratificaron que la ciberdefensa es uno de los principales elementos de la defensa colectiva, siendo también importante en las otras dos *core tasks* de la OTAN: gestión de crisis y la seguridad cooperativa. También se comprometieron a desarrollar las capacidades necesarias para proteger sus ciberespacios nacionales y, siguiendo la senda planteada por el *Manual de Tallin*[10], se determinó que el Derecho Internacional también es aplicable al ciberespacio. Igualmente, para zanjar los debates surgidos en los años anteriores sobre la activación del Artículo 5 del Tratado de Washington en caso de ciberataque y la dificultad práctica de implementar esta decisión, los veintiocho acordaron que la respuesta colectiva se produciría tras examinar el ataque caso por caso. Finalmente, los gobiernos aliados acordaron mejorar la cooperación con la industria, la compartición de información y la asistencia mutua y el adiestramiento y ejercicios, sentando las bases de la denominada *Ciberdefensa 3.0*.

Tras la Cumbre, la Alianza procedió a reforzar sus lazos con la industria lanzando el *NATO Industry Cyber Partnership* (NICP), una iniciativa que busca ahondar en formas de colaboración público-privada para generar –tal y como ha reconocido explícitamente Estados

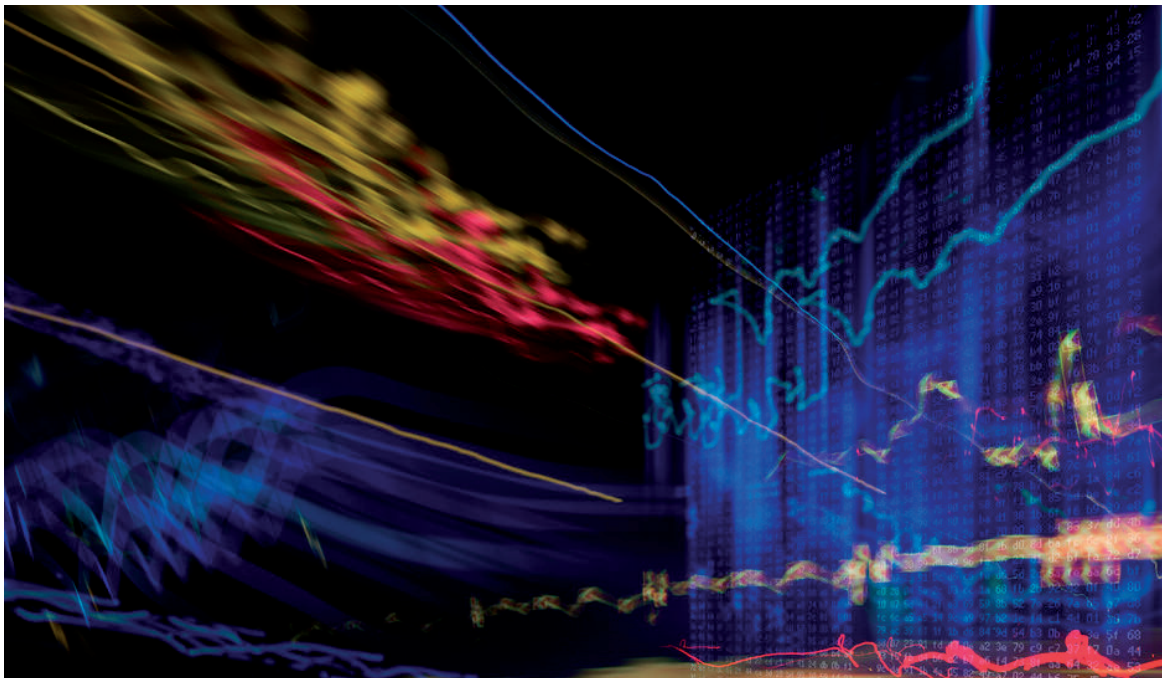
Unidos con la Iniciativa de Innovación en Defensa para apoyar tecnológicamente la Tercera Estrategia de Compensación y la Unidad Experimental de Innovación en Defensa (DIUx) para estrechar lazos con *Silicon Valley*– las cibercapacidades requeridas por la OTAN y sus socios. También hizo lo mismo con la Unión Europea que, inmersa en su propio proceso de construcción de cibercapacidades para no quedarse rezagada de la Era de la Información y apoyar la consolidación de la Política Común de Seguridad y Defensa (PCSD), culminó el pasado febrero con la firma de los *Acuerdos Técnicos en Ciberdefensa* para facilitar el intercambio de información relevante sobre ciberamenazas y ciberincidentes entre los equipos de respuesta de ambas organizaciones. A tenor de la declaración final de la Cumbre de Varsovia, es de esperar que los lazos con la industria y con la Unión Europea se incrementen en los próximos meses[11].

Finalmente, en el mes de julio se celebró en la capital polaca la última Cumbre de la Alianza. Reconociendo *"…que el ciberespacio es un dominio de las operaciones en el cual la OTAN debe defenderse tan efectivamente como lo hace en el aire, en la tierra o en el mar […] y conducir operaciones en estos dominios manteniendo nuestra libertad de acción y decisión"*[12] y que cualquier acción cibernética deberá ser acorde al Derecho Internacional, los líderes aliados establecieron que el ciberespacio sería el cuarto dominio del entorno operativo, y no el quinto, como asume Estados Unidos. Esta decisión no solo tiene dos importantes lecturas: una política, al reconocer explícitamente –quizás forzada por la creciente asertividad de Moscú en esta dimensión en forma de ciberataques, ciberpropaganda, ingeniería social o ciberespionaje y su integración tanto en su acción exterior como en acciones híbridas– que lo "ciber" es un elemento consustancial en la guerra moderna. Y otra operativa, avanzando en su integración tanto en el planeamiento y conducción de operaciones, la generación de capacidades, la gestión de los recursos y los planes de transformación. En este sentido, en Varsovia se volvió a recordar que si bien la Alianza apuesta decididamente por el desarrollo de cibercapacidades, los responsables de mejorar la capacidad de detección, respuesta, defensa y resiliencia de sus redes e infraestructuras nacionales son los miembros de la organización.

En definitiva, aunque en la capital polaca se ha dado un nuevo impulso al desarrollo de la ciberdefensa aliada, todavía quedan dos grandes cuestiones pendientes: por un lado, homogeneizar las cibercapacidades de los estados miembros. Recuérdese que las capacidades

aliadas cubren las necesidades operativas del Cuartel General, la estructura de mandos y los organismos asociados, estando subsidiariamente a disposición de los miembros, lo que hace necesario que sean los mismos países los que desarrollen sus propias capacidades de ciberdefensa y mejoren la resiliencia de sus redes y sistemas. Sin embargo, el nivel de madurez tecnológica, organizativa o doctrinal de los veintiocho en esta materia es muy heterogénea y proporcional a su capacidad de asimilar la importancia estratégica que tiene este dominio. Aunque en Varsovia se ha emplazado el ciberespacio como uno de los cuatro dominios de las operaciones aliadas –tras el aire, la tierra y los mares– y se ha reconocido su importancia intrínseca para la defensa colectiva, la gestión de crisis y la seguridad cooperativa, varios países están afrontando su adaptación al ciberespacio desde la urgencia, sin un convencimiento o conocimiento real de su valor y con resistencias corporativas a la innovación. Precisamente, esta misma heterogeneidad en materia de cibercapacidades está motivando que algunas de las principales potencias cibernéticas de la Alianza Atlántica se muestren reticentes a cooperar en el desarrollo de capacidades, desvelar su arsenal cibernético e incluso a emplearlo en caso de ciberataque.

Por otro lado, definir los límites del Artículo 5 del Tratado de Washington: la OTAN todavía no ha detallado qué podría constituir un ciberataque ni tampoco ha determinado el umbral a partir del cual un ataque de estas características debería ser calificado como una agresión contra un estado miembro y, por tanto, susceptible de motivar la activación de la respuesta colectiva. Aunque durante la reunión de los ministros de Defensa de junio de 2016 el secretario general Jens Stoltenberg declaró que un ciberataque severo podría ser constitutivo de una respuesta colectiva[13], es preciso recordar que cualquier acto de estas características contra un miembro de la OTAN será analizado caso por caso por el Consejo del Atlántico Norte –quizás considerando la tipología de actor y la amplitud, duración, intensidad del mismo– y no supondrá la activación automática del Artículo 5. Del mismo modo, determinar la atribución de un ciberataque continúa siendo el principal problema que debe afrontar la Alianza en este ámbito, puesto que hoy en día no es posible desde un punto de vista tecnológico determinar con certeza y celeridad la procedencia de un ciberataque y la responsabilidad última del mismo, especialmente cuando éstos pueden realizarse a través de terceros (*proxies*). En este sentido, aunque la OTAN está barajando la atribución por asimilación (fijando la autoría del ataque por el contexto de la crisis), mejorando la protección y resiliencia de sus redes e infraestructuras (para incrementar la disuasión por negación, puesto que para la disuasión por castigo requeriría desarrollar capacidades ofensivas) y diseñando un catálogo de opciones de respuesta (cibernética, convencional o mixta), cabe preguntarse si un ciberataque presumiblemente realizado por una potencia adversaria implicaría una respuesta real y colectiva. Quizás, la respues-



ta pasará por continuar con estos desarrollos doctrinales mientras se habilita el mecanismo de consultas previsto en el Artículo 4 del Tratado de Washington para que los miembros que sufran un ciberataque puedan recibir una cierta solidaridad del resto de los países y escalar políticamente antes de arriesgarse a solicitar la invocación del Artículo 5.

En conclusión, a pesar de que la ciberdefensa se ha consolidado definitivamente en la Alianza Atlántica, son muchos los estados miembros que todavía no disponen del mínimo de capacidades para identificar, protegerse, reponerse –y mucho menos responder– en caso de ciberataques. La ciberdefensa ha erosionado el principio de solidaridad en la OTAN y ha provocado una nueva brecha de capacidades, por lo que es esencial que los países desarrollen capacidades específicas porque difícilmente podrán valerse de los medios propios de la organización o aprovecharse de las capacidades del resto de los miembros, reticentes a revelar sus medios y críticos con las estrategias de *free-rider* de varios de los aliados. Otro importante reto para la organización. •

NOTAS

[1]Trine Flockhart: *Preparing for NATO's Warsaw Summit: the Challenges of Adapting to Strategic Change*, DIIS Report 2015-16, Copenhagen: Danish Institute for International Studies, 2015.

[2]Ellen Mesmer: "Serb supporters sock it to NATO, U.S. Web sites", *Cable News Network* (6 de abril de 1999).

[3]Wayne Larsen: *Serbian Information Operations During Operation Allied Force,* Maxwell AFB: Air Command & Staff College, 2000.

[4]Este acuerdo pretendía que los socios se comprometieran a mejorar sus capacidades propias en áreas consideradas esenciales (transporte estratégico, reabastecimiento en vuelo, apoyo al combate, sistemas C^{3}I, medios de observación táctica y estratégica, armas de precisión, sistemas de supresión de defensas aéreas, equipos de defensa nuclear, biológica, química o radiológica o un sistema de defensa antimisiles de teatro), en los plazos concretos y manteniendo un alto grado de supervisión en su implementación.

[5]Stephen Herzog: "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses", *Journal of Strategic Security*, Vol. 4 Núm. 2, 2011, pp. 49-60.

[6]Declaración final de la Cumbre de Bucarest (3 de abril de 2008), para. 47.

[7]Guillem Colom: "La Alianza Atlántica ante el nuevo Concepto Estratégico", *Revista de Estudios Europeos*, Núm. 59, 2012, pp. 41-60.

[8]Este asunto –países que se aprovechan de la defensa colectiva y del poder norteamericano para reducir su gasto en defensa y contribuir menos a los objetivos de la organización– es un tema recurrente y ampliamente analizado en la literatura académica. James Murdoch y Todd Sandler: "Complementarity, free riding, and the military expeditures of NATO allies", *Journal of Public Economics*, Vol. 25, Núm. 1-2, 1984, pp. 83-101.

[9]Fernando Gualdoni: "La ciberdefensa socaba la unidad de la OTAN", *El País* (23 de octubre de 2013).

[10]Michael Schmitt (ed.): *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Tallin: NATO CCD-CoE, 2013.

[11]Declaración final de la Cumbre de Varsovia (9 de julio de 2016), para. 71.

[12]*Ibíd.*, para. 70.

[13]Andrea Shalal: "Massive cyber attack could trigger NATO response: Stoltenberg", *Reuters* (16 de junio de 2016).