Comentario THIBER:

Trump y la Ciberdefensa Aliada

AUTOR: Guillem Colom Piela, director de THIBER

Desde la entrada de Donald Trump en la Casa Blanca, las crónicas sobre la OTAN se centran en las agrias críticas del presidente estadounidense a sus socios europeos por la falta de compromiso con la seguridad euroatlántica y la necesidad de que éstos inviertan más en defensa. En la pasada Cumbre de Bruselas, celebrada en la capital belga en julio de 2018, sucedió algo similar. Sin embargo, además de la solicitud de Trump de alcanzar un 4% – doblando el objetivo establecido en la Cumbre de Gales cuatro años antes – del Producto Interior Bruto (PIB) en gasto militar, se trataron muchos otros asuntos como la asertividad rusa en su área de influencia, sus actuaciones en la zona gris o las operaciones de información sobre sociedades y procesos electorales extranjeros, la cooperación entre la Alianza Atlántica y la Unión Europea o la necesidad de desarrollar la ciberdefensa.

A diferencia de encuentros anteriores, en Bruselas no se lograron grandes avances en esta materia y las crónicas se centraron en los objetivos de gasto. Sin embargo, a finales de 2018 Estados Unidos planteó poner a disposición de la OTAN sus cibercapacidades, una propuesta que sería asumida por otras potencias aliadas. Esta decisión no sólo parece demostrar que, más allá de la retórica incendiaria de Trump, Washington continúa comprometido – quizás, más que muchos países europeos – en la seguridad euroatlántica, sino también supone un punto y a parte en la ciberestrategia aliada.

Desde que la Alianza Atlántica empezara a construir su arquitectura de ciberseguridad tras la Cumbre de Praga, se asumió que ésta sería de naturaleza puramente defensiva y se orientaría a la protección de sus redes y sistemas, siendo

Estados Unidos planteó poner a disposición de la OTAN sus cibercapacidades, incluidas las ofensivas, una propuesta que sería asumida por otras potencias aliadas

responsabilidad de los distintos países la protección y modernización de sus medios. Aunque su Secretario General ha planteado repetidamente la conveniencia de integrar las cibercapacidades – incluyendo las de naturaleza ofensiva – de sus miembros en las operaciones militares para disuadir, repeler y protegerse de las amenazas, el tabú del desarrollo de capacidades y estrategias puramente ofensivas continúa existiendo en la actualidad. Sin embargo, a pesar de las controversias políticas y la brecha de capacidades que existe entre sus miembros, el ofrecimiento estadounidense es muy significativo porque representa una solución de compromiso si no se quiere levantar políticamente este tabú.

Condicionada por las actividades cibernéticas e informativas rusas, chinas o iraníes, la *Ciber Estrategia* que el Pentágono presentó el pasado septiembre proponía acometer una "defensa avanzada" con la finalidad de *"...degradar o detener actividades cibernéticas en su origen, incluyendo cualquier actividad que se encuentre por debajo de un conflicto armado* [lo que viene llamándose la zona gris, el amplio espacio situado entre la paz y las hostilidades abiertas]". En otras palabras, aunque la "defensa avanzada" es de naturaleza defensiva, su ejecución supone que las infraestructuras cibernéticas de otro país puedan convertirse en un objetivo a la hora prevenir un ciberataque.

Aunque esta decisión estadounidense no incrementará necesariamente la capacidad de ciberdisuasión de la OTAN, si proporcionará más resiliencia contra los ciberriesgos y mejorará la credibilidad de la organización en el ciberespacio. Además, interfiriendo en las acciones adversarias, se podrá anticipar y prevenir ataques sobre los países miembros. Aunque estos cambios podrían motivar hipotéticas escaladas, quizás el mayor riesgo radica en que varios miembros podrán verse tentados a adoptar estrategias de *free-rider* y no desarrollar cibercapacidades propias, ampliando nuevamente la brecha militar entre los aliados y dando la razón a Donald Trump.