Tanto la Brújula Estratégica como el nuevo concepto estratégico de la Alianza analizan las armas cibernéticas y aportan respuestas ante un posible ataque

La UE y la OTAN ante los nuevos escenarios de la seguridad y la defensa

Teniente coronel Dr. Fernando Noguera Gómez, Dra. Dolores Fuensanta Martínez Martínez, Dra. María Magdalena Fernández Valera y Dra. María Concepción Pérez Cárceles
Profesores del Centro Universitario de la Defensa de la Academia General del Aire

La generalización del uso de internet y las nuevas tecnologías son una realidad que ha cambiado la sociedad de nuestros días. La dependencia digital entraña nuevos peligros que deben conocerse. La vulnerabilidad de las comunicaciones o de la misma privacidad son un pequeño indicio de los riesgos de la hiperconectividad. De hecho, instituciones del más alto nivel como el Fondo Monetario Internacional identifican claramente esta amenaza que ya han incluido en su último informe anual de enero de 2022: «En la medida que la sociedad continúa migrando al mundo digital, la amenaza del cibercrimen se cierne sobre el terreno. Esta situación genera no solo un coste financiero para las organizaciones, sino que también se advierte del peligro para las infraestructuras críticas, la cohesión de la sociedad y el propio bienestar mental de los ciudadanos».

Este artículo aborda el planeamiento estratégico general sobre seguridad y defensa en el entorno de las dos principales organizaciones internacionales regionales a las que pertenece España. No obstante, con carácter previo, se plantea una aproximación al concepto de ataque armado en el ciberespacio como eje central de los nuevos escenarios de la defensa.

Por un lado, la Organización del Tratado del Atlántico Norte como alianza pionera específicamente político-militar, en la reciente cumbre de Madrid, ha adoptado un nuevo Concepto Estratégico que llega a considerar el ciberataque como ataque armado susceptible de activar los mecanismos solidarios de defensa. Por otro lado, la UE en el Consejo Europeo celebrado el 24 y 25 de marzo del 2022 ratificó la Brújula Estratégica. Se trata de un nuevo impulso en el proceso de construcción de una auténtica Política Común de Seguridad y Defensa (PCSD). Estrategia alineada en todo momento con los procesos de la OTAN, también supone el reconocimiento de la capacidad defensiva de la Unión Europea y de su autonomía estratégica como potencia global que por su fuerza económica y política le corresponde. El ciberespacio se considera el nuevo escenario de la competencia estratégica. Al igual que se garantiza el acceso seguro a ámbitos estratégicos clásicos como el alta mar, el ámbito aéreo y el espacio, requiere instrumentos específicos de ciberdefensa como lo son las intervenciones en respuesta a las amenazas híbridas y/o, en su caso, un despliegue militar rápido de la Unión Europea.

NUEVOS ESCENARIOS

Los principales riesgos y amenazas de seguridad y defensa a los que se enfrenta una sociedad geopolítica y tecnológicamente en constante mutación provienen del ciberespacio. Es el eje central de los nuevos escenarios de competencia estratégica como reconoce la UE. En primer lugar, el ejercicio de la legítima defensa individual o colectiva por parte de un Estado ante un ataque armado es un derecho reconocido en el artículo 51 de la Carta de Naciones Unidas. No obstante, analizar el significado de un ataque armado exige un recorrido por los diferentes compromisos acordados por la comunidad internacional. En el año 1974, la resolución 3314 de la Asamblea General de la Naciones Unidas definió en su artículo 1 el concepto de agresión como «el uso de la fuerza armada por un Estado contra la soberanía, la integridad territorial o la independencia política de otro Estado, o en cualquier otra forma incompatible con la Carta de las Naciones Unidas». Esta primera aproximación reconoce el derecho de un Estado a defenderse cuando es objeto de un ataque por parte de otro Estado.

En segundo lugar, es preciso detenerse en el concepto de ataque armado para estudiar posteriormente su trasposición al ciberespacio.

Los principales riesgos de una sociedad en constante mutación provienen del ciberespacio

El Derecho Internacional Humanitario establece en el artículo 49 del I Protocolo Adicional a los Convenios de Ginebra que: «se entiende por ataques los actos de violencia contra el adversario, sean ofensivos o defensivos. (…) se aplicarán a cualquier operación de guerra terrestre, naval o aérea que pueda afectar en tierra a la población civil, a las personas civiles y a los bienes de carácter civil».

A pesar de todo ello, la aplicación práctica del artículo 2.4 de la Carta de la ONU sigue siendo motivo de controversia. Es complicado definir a partir de dónde se considera un ataque armado o qué requisitos debe tener. Diferentes autores se han pronunciado sobre en qué momento un acto se convierte en un ataque armado. En este sentido, el académico estadounidense experto en derecho internacional aplicable al ciberespacio Michael N. Schmidt entiende que cuando los tradicionales ataques dinámicos pueden calificarse como ataques armados, también pueden serlo aquellos ataques cibernéticos que causen daños o perjuicios (artículo *The Law of Cyber Warefare: Quo Vadis?* publicado en la revista jurídica de la Universidad de Stanford).

En el caso de España, el Mando Conjunto de Ciberdefensa definió el concepto de ciberataque como: la «acción producida en el ciberespacio que compromete la disponibilidad, integridad y confidencialidad de la información mediante el acceso no autorizado, la modificación, degradación o destrucción de los sistemas de información y telecomunicaciones o las infraestructuras que los soportan» (orden ministerial de 19 de febrero de 2012 por la que se crea el Mando Conjunto de Ciberdefensa).

LA BRÚJULA ESTRATÉGICA

El compromiso de la UE para la seguridad y defensa común se ha diferenciado del resto de los logros comunitarios. Un recorrido caracterizado por luces y sombras que llega hasta nuestros días. Se inició con el Tratado de Bruselas del año 1948 y con la creación de la Unión Europea Occidental como organización militar en el año 1957.

Con el Tratado de la Unión Europea o Tratado de Lisboa del año 2010 se produce un verdadero punto de inflexión en este recorrido. En primer lugar, supuso la disolución de la UEO y, además, significó la separación de la Acción Exterior del resto de políticas de la Unión. Nace así una Política Europea de Seguridad Común (PESC), donde la UE se atribuye una personalidad jurídica propia y una única voz en el ámbito de las relaciones internacionales.

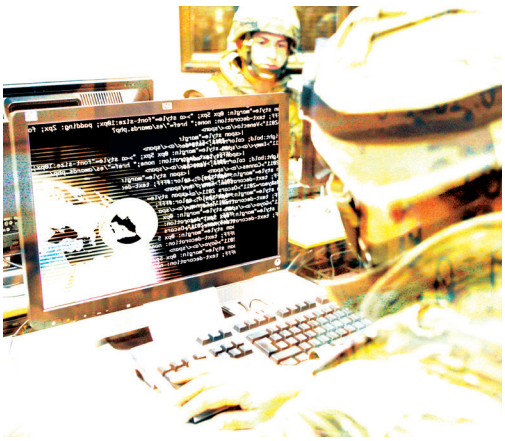
La PESC incluye a su vez a la Política Común de Seguridad y Defensa. Así, en virtud a este importante Tratado de Lisboa, se creó una cláusula de defensa mutua como elemento clave de la PCSD que ofrece a la Unión una capacidad operativa basada tanto en medios civiles como militares. La cláusula de defensa mutua recogida en artículo 42.7 del Tratado de la Unión establece: «Si un Estado miembro es objeto de una agresión armada en su territorio, los demás Estados miembros le deberán ayuda y asistencia con todos los medios a su alcance, de conformidad con el artículo 51 de la Carta de las Naciones Unidas. Ello se entiende sin perjuicio del carácter específico de la política de seguridad y defensa de determinados Estados miembros».

A la vista de estos antecedentes, la Brújula Estratégica de la UE se convierte en el siguiente hito hacia una Europa más unida también en el ámbito de la seguridad y la defensa. Desde el inicio del documento se reconoce la necesidad de anticipación ante las amenazas, garantizar un acceso seguro a los ámbitos estratégicos y proteger a nuestros ciudadanos. Por ello, textualmente establece que: «crearemos un conjunto de instrumentos de la UE contra las amenazas híbridas que reúna diferentes herramientas para detectar una amplia gama de amenazas híbridas y responder a ellas. En este contexto, desarrollaremos un conjunto de instrumentos específicos para hacer frente a la manipulación de información y la injerencia por parte de agentes extranjeros. Seguiremos desarrollando la política de ciberdefensa de la UE para estar mejor preparados ante los ciberataques y responder mejor a ellos».

En suma, esta iniciativa supone un compromiso más firme y concreto en el ámbito de la PCSD, con un plan de acción específico en el nuevo escenario del ciberespacio que se analiza. En particular, se tiene previsto la creación de un Núcleo de Innovación en Defensa, un Observatorio sobre tecnologías críticas y una Agencia de Investigación Estratégica Global.

EL PLANEAMIENTO DE LA OTAN

Desde sus orígenes la OTAN se ha configurado como garante de la integridad territorial de sus miembros. Así en el Tratado de Washington suscrito en 1949 destaca el importante artículo 5 que establece: «Las Partes acuerdan que un ataque armado contra una o más de ellas, que tenga lugar en Europa o en América del Norte, será considerado como un ataque dirigido contra todas ellas, y en consecuencia, acuerdan que si tal ataque se produce, cada una de ellas, en ejercicio del derecho de legítima defensa individual o colectiva reconocido por el artículo 51 de la Carta de las Naciones Unidas, ayudará a la Parte o Partes atacadas, adoptando seguidamente, de forma individual y de acuerdo con las otras Partes, las medidas que juzgue necesarias, incluso el empleo de la fuerza armada, para restablecer la seguridad en la zona del Atlántico Norte.(…)».



Rafa Navarro

Recientemente, en la Cumbre de Madrid de junio de 2022, se aprueba el nuevo concepto estratégico de la OTAN. Hay que señalar que entre sus objetivos concretos establece «mantener el uso seguro y el acceso sin restricciones al espacio y al ciberespacio es clave para una disuasión y defensa eficaces». Se trata de un documento muy completo en el que reconoce a Rusia como la amenaza más significativa y directa para la seguridad de los aliados y para la paz y la estabilidad en la zona euroatlántica y también el desafío que supone China. Señala que el propósito fundamental de la capacidad nuclear de la OTAN es preservar la paz. Respecto al flanco Sur reconoce que los conflictos afectan directamente a su seguridad, y por último, respecto a la integridad territorial se compromete «a defender cada centímetro cuadrado» de los socios aliados.

Profundizando en el ámbito de la ciberseguridad y reconociendo la situación expuesta anteriormente, se comprometen a acelerar la transformación digital, adaptar la estructura de Mando de la OTAN para la era de la información y mejorar las ciberdefensas, redes e infraestructuras. También insiste en la seguridad colectiva recordando la estrecha conexión con la Unión Europea con la que comparte valores comunes. Así propone mejorar la estrategia OTAN-UE en cuestiones de interés común que entre otras son las tecnologías emergentes y disruptivas.

Para finalizar se propone destacar un aspecto que puede resumir gran parte de este artículo. En concreto la Alianza reconoce que las operaciones híbridas contra los aliados podrían alcanzar el nivel de ataque armado. En este punto se solucionan las dudas sobre el carácter armado o no de una agresión en el ciberespacio. La propia Alianza eleva el carácter armado explícitamente. Más aún si cabe, claramente señala que el Consejo del Atlántico Norte podría invocar el artículo 5 del Tratado del Atlántico Norte (seguridad colectiva y solidaria).

CONCLUSIONES

La transformación de la sociedad que supone la revolución digital tiene también consecuencias en la seguridad de los países de nuestro entorno. Supone la aparición de nuevas amenazas desconocidas hasta la fecha que utilizan el ciberespacio como medio necesario para su propagación.

La consideración de un ciberataque como agresión supone la legitimación de la respuesta por parte del Estado atacado. Se trata de un supuesto que se puede incluir dentro del artículo 51 de la Carta de Naciones Unidas que establece los requisitos de la legítima defensa. Así se podría plantear la identificación de los tradicionales ataques dinámicos, calificados como ataques armados, con aquellos ataques cibernéticos que causen daños o perjuicios.

La legítima defensa colectiva se reconoce también por la comunidad internacional y se puede incluir en la regulación de las diferentes organizaciones internacionales. Este es el caso de la Unión Europea que, tras un largo proceso, en el Tratado de Lisboa incorpora la cláusula de defensa mutua como elemento clave de la PCSD. Ofrece a la Unión una capacidad operativa basada en medios civiles y militares. En esta línea, la Brújula Estratégica recientemente aprobada por el Consejo Europea establece unos compromisos concretos. Entre ellos destacan diversas iniciativas en ciberdefensa.

Por su parte, la OTAN en su también reciente cumbre celebrada en Madrid formaliza un nuevo Concepto Estratégico. La evolución del planeamiento estratégico se ha ido adaptando a la situación geopolítica de los Estados miembros. Así desde la Guerra Fría como principal amenaza se llega a un mundo hiperconectado. Según el Concepto Estratégico: «Un acto aislado o un conjunto de actividades maliciosas cíber, o bien una operación hostil hacia, desde o en el espacio, podría alcanzar el nivel de un ataque armado y llevar al Consejo del Atlántico Norte a invocar el artículo 5 del Tratado del Atlántico Norte».

Para concluir, la seguridad y defensa del nuevo escenario operativo del ciberespacio, requiere de una acción conjunta y cooperación supranacional entre Estados aliados. La Brújula Estratégica de la UE y el nuevo Concepto Estratégico de la OTAN bien podrían ser consideradas, con carácter general, como las dos caras de una misma moneda. Se trata de la consecución del objetivo común del mantenimiento de la paz internacional y defensa de los intereses y valores de sus ciudadanos.