La ciberdefensa en el ámbito de la OTAN

Rubén C. García Servert
Teniente general (EA)
Comandante del Centro de Operaciones Aéreas Combinadas Sur de la OTAN
Academia de las Ciencias y las Artes Militares

Lino Iglesias Posada
Teniente coronel (EA)
Jefe de la Agencia OTAN de Comunicaciones e Información en España

La ciberdefensa en la OTAN: ¿un problema de concepto?

Desde su aparición y dadas sus características inherentes, la amenaza en el ciberespacio ha supuesto primero una incertidumbre y luego un replanteamiento de paradigmas de conflicto. La misión de la Alianza incluye, sin duda, ser capaz de defenderse en el ciberespacio, de la misma manera que lo hace en los demás dominios, terrestre, marítimo, aéreo... Pero el ciberespacio no es un dominio como los demás, pues es terreno de intrínseca asimetría de los bandos en conflicto. Por ello, la respuesta de la Alianza queda condicionada a la existencia de indicadores muy certeros sobre la autoría de los ataques, concepto que se desarrollará más adelante cuando tratemos sobre la atribución. En ausencia de estos indicadores, se abriría la puerta a un peligroso juego de respuestas indiscriminadas, de consecuencias insospechadas.

Otra cuestión compleja es la previsibilidad de los efectos, en el tiempo y en su magnitud, esencial, pero difícil de alcanzar en esta materia o la exigencia de un conocimiento cabal de

las motivaciones del adversario, sean «tradicionales» por su impacto estratégico como la búsqueda de efectos económicos, la desestabilización político-social de una región o bien más «innovadores» como la necesidad de notoriedad de un individuo u organización, la difamación o la venganza, que pueden ocasionar efectos globales de riesgos para la seguridad o estabilidad de una determinada región o colectivo social.

De ahí que, en la cumbre de Varsovia de 2016, la OTAN diera un paso al frente en el tratamiento y la respuesta de estas amenazas al producir la «*Cyber Security Pledge»* (promesa en materia de ciberseguridad) con la que los países firmantes se comprometieron a llevar a cabo medidas que incrementasen la resiliencia de los medios nacionales en materia de ciberdefensa como contribución esencial a la Defensa Colectiva (valor fundamental de la Alianza junto a la Gestión de Crisis y la Seguridad Cooperativa).

El caso particular de la atribución de un ataque:

Visto lo anterior, la naturaleza esencial de la OTAN, como Alianza defensiva sigue en vigor, así como su fiel adherencia a leyes y tratados internacionales. Estos dos elementos condicionan todos los planteamientos y estrategias aliadas. El uso de capacidades ofensivas por parte de la Alianza no está limitado, pero sí ha de ser coherente con los principios anteriores.

Se abre aquí la polémica del primer ataque o la renuncia a ataques preventivos, en los mismos términos que pueden aplicarse a los otros dominios. En la actualidad disponen de capacidades ofensivas ciertos estados (9 en la actualidad), que las han declarado en el marco del acuerdo SCEPVA (Ciber-Efectos Soberanos Proporcionados Voluntariamente por los Aliados), acuerdo que presenta una vulnerabilidad muy notoria dado que se basa en la confianza y la confidencialidad de éstos.

De lo anterior se deduce que, la aplicación del art. 5 del Tratado de Washington (Defensa Colectiva) en el dominio ciber estaría condicionada a que las acciones de la otra parte se considerasen como ofensivas contra uno o más de los Estados aliados y que pudiesen ser atribuidas a una organización Estatal, que se enmarcase en un territorio geográfico definido o que fuese financiado o apoyado por éste. Se trata de hacer aplicables los requisitos de la legítima defensa al ámbito cíber.

Volviendo al marco legal, cabe decir que el Derecho Internacional actual que regula las relaciones entre Estados, no pone límites a las actuaciones en su territorio más allá de que no se violen desde el territorio propio la soberanía ni la integridad de otro Estado, y exige la diligencia debida para que no permita el empleo de su territorio o de sus infraestructuras para acciones dirigidas a infligir consecuencias que afecten gravemente al funcionamiento de las infraestructuras críticas o supongan un impacto significativo en la economía de un tercero.

Es responsabilidad de los Estados la realización u omisión de actos que constituyan una ruptura de esta obligación internacional, siendo atribuible a ese Estado las actuaciones realizadas desde su territorio. Hay aquí una obligación que va más allá del deber de abstención de acciones ofensivas y que exige controlar lo que ciudadanos y organizaciones realicen desde su territorio.

Nacimiento del Centro de Operaciones de Ciberdefensa (en adelante CyOC)

El CyOC de la OTAN situado en Mons (Bélgica) nace en 2018 como consecuencia de la necesidad de disponer de una capacidad de defensa sólida en el ciberespacio que concrete el compromiso de la Alianza con la defensa colectiva en el nuevo dominio. Se trata de disuadir a adversarios potenciales, así como asegurar la capacidad de desarrollar las misiones encomendadas en y a través del ciberespacio, tanto en periodos de paz, crisis o conflicto, para proporcionar información válida sobre el entorno y coordinar las actividades operativas OTAN en el ciberespacio. En el último trimestre de 2019 alcanza su primer hito operacional con la consecución de la Capacidad Operacional Inicial (IOC), teniendo prevista su Capacidad Operacional Plena (FOC) en 2023.

Creación del NCSC (NATO Cyber Security Center)

Nace en 2019 fruto de la evolución del Centro de Respuesta a Incidentes Informáticos en la OTAN (NCIRC), no solo como el organismo responsable de defender las redes de mando, control y comunicaciones (en adelante C3) de la OTAN, sino también con el objetivo de permitir a la Alianza llevar a cabo de manera segura la conducción de operaciones y misiones.

Sus principales características son la monitorización centralizada de las redes de comunicaciones, mando y control de la Alianza y la capacidad de respuesta a incidentes en el entorno OTAN, que no olvidemos que se compone de una comunidad superior a los 100.000 usuarios en más de 50 localidades. Por poner un ejemplo, que da idea de la magnitud de la entidad, el NCSC analiza y guarda más de 20TB (terabytes) de información al día.

Pero el NCSC no se reduce solo a tareas de prevención y defensa de estas redes de C3 OTAN, sino que por medio de herramientas de control extrae datos que le permite realizar la labor de apoyo a la toma de decisiones a las altas instancias OTAN que incluyen a su Secretario General, está plenamente integrado en los procesos de planeamiento de operaciones y ejercicios OTAN y ha creado entorno a sí una red de colaboración con entidades nacionales o supranacionales.

Ejemplos de ello son:

- El *«NATO Industry Cyber Partnership»*, que vio la luz en la cumbre de Gales de 2014 para fomentar que la Alianza sacase provecho de la innovación tecnológica y la experiencia del sector privado en orden a la consecución de los objetivos de una política de defensa mejorada de ciberdefensa o,
- El Acuerdo Técnico firmado en febrero de 2016 entre el NCIRC (hoy día NCSC) y los Equipos de Respuesta ante Incidentes Informáticos de la Unión Europea (CERT-EU) para fomentar compartir la información en esta materia y hacer un mejor uso de los recursos disponibles.
- Para desempeñar estas misiones, el NCSC cuenta con más de 2000 expertos dentro de la Agencia de Comunicaciones e Información de la OTAN (NCIA), con una capacidad de despliegue en cualquier escenario, incluidos los teatros de operaciones, de hasta dos equipos de respuesta, previa aprobación del Consejo del Atlántico Norte (NAC).

Los principales temas a debate en el Dominio Ciberespacial, a fecha de hoy.

La declaración doctrinal del ciberespacio como quinto dominio operacional obliga, no obstante, a evoluciones conceptuales y prácticas en esta materia. Las definiciones y los conceptos no están del todo asentadas y, por ello, parece esencial el debate, entre otras, de las siguientes cuestiones de diversa naturaleza, algunas de las cuales ya han sido apuntadas en los apartados anteriores:

- Conceptuales, como el salto desde una ciberdefensa (totalmente alineada con la postura defensiva de la OTAN) a ciberoperaciones (que incluyan operaciones ofensivas) en este dominio, lo cual obliga a un control político estrecho de estas novedosas actuaciones.
- Orgánicas y Operativas, como la formalización del dominio cíber y de las ciberoperaciones en las estructuras aliadas de Mando y Control, incluyendo la necesaria activación de Mandos Componentes Cíber a nivel táctico en toda operación conjunta, con una dependencia orgánica del Mando Conjunto Operacional responsable.
- Jurídicas como la ya comentada necesidad de atribución del origen de un ataque para dar legitimidad a una contra respuesta ofensiva, más allá de la mera defensa propia, que quedaría amparada por el artículo 51 de la Carta de las Naciones Unidas.
- Existenciales, como la muy polémica consideración de un ciberataque como un supuesto que pudiera dar lugar a la invocación del artículo quinto del Tratado de Washington, con un correlato nuclear. Hay aquí una interpretación forzada del «supuesto de ataque al territorio aliado» que pudiera dar lugar a graves disensiones entre los aliados y a una más que dudosa coherencia con la legalidad internacional.

En resumen, más allá del hecho de que nos encontramos ante un nuevo dominio operacional y a la constatación de la existencia de actores (no necesariamente estatales) que recurren

sistemáticamente a operaciones ofensivas cíber, parece claro que, además de las capacidades técnicas, se abre un interesante debate jurídico y estratégico al que conviene prestar atención.

Conclusiones.

Como se puede ver en este breve artículo, nos encontramos ante un escenario complejo con múltiples actores, no necesariamente Estados, y con un problema persistente de identificación del adversario por parte de quien recibe el ataque. Se trata sin duda de un nuevo dominio para las operaciones.

Los ataques, dependiendo de la escala e intención, pueden ir desde una mera suplantación de la identidad hasta una degradación grave o negación en la provisión de servicios básicos, pudiendo incluso afectar a las infraestructuras críticas. Por ello es necesario contar con una estructura que proporcione una vigilancia constante del dominio del ciberespacio, y que garantice, amparada por el Derecho Internacional, el Derecho Internacional de los Derechos Humanos y el Derecho de los Conflictos Armados la seguridad y el bienestar de los ciudadanos y el empleo libre, seguro de las redes de C3 y de las infraestructuras soberanas.

Lo más reconfortante es que la OTAN ha evolucionado desde 2015 desarrollando una estructura robusta que va desde el desarrollo de procedimientos, la creación de estructuras tanto de nivel de dirección o planificación estratégicas o el establecimiento de herramientas ejecutivas para acometer las nuevas amenazas que asedian a sus miembros.