LA COLABORACIÓN ENTRE LA OTAN Y LA UE EN EL ÁMBITO DEL CIBERESPACIO: SITUACIÓN ACTUAL Y PROYECTOS CONJUNTOS

VICENTE GONZALVO NAVARRO

Coronel de Infantería de Marina

La evolución de la concepción del ciberespacio en la OTAN y la UE ha sido variopinta y similar al mismo tiempo en estas dos organizaciones. Me explicaré: Ha sido variopinta porque la OTAN ha centrado su desarrollo en la aplicación militar del ciberespacio mientras la UE se ha orientado más en el desarrollo de las capacidades ciber en la sociedad civil; y similar porque el desarrollo de esta capacidad ha seguido unas pautas, en cierto modo, análogas como veremos.

En ese sentido, y para determinar, y facilitar la comprensión sobre el nivel de desarrollo de los conceptos, estrategias y herramientas en relación con el ciberespacio (al respecto de la OTAN y de la UE), y la situación actual de la cooperación en este ámbito entre ambas, definiriremos una serie de hitos (generales y que pueden no ser totalmente precisos) pero que considero ayudan a delimitar la situación actual de (y sobre) estos asuntos.

De manera que, tras realizar esta evaluación, nos sea posible realizar una estimación de la evolución y de la situación actual de la cooperación OTAN-UE en relación al ciberespacio. Sin querer en ningún caso pontificar, estas posibles referencias o hitos generales podrían ser temporal y sucesivamente (1): «beginning» (el comienzo), «founding» (la fundación y desarrollo de principios), «centralizing» (la centralización y coordinación), «enhancing» (la promoción y desarrollo), «operating» (la obtención de la capacidad operativa) y «shaping» (la adecuación y definición final) (2).

LA OTAN Y LA UE

En concreto, para la OTAN, este proceso de evolución (en sucesivas Cumbres o declaraciones políticas) comenzó en el año 2002 (no hace tanto efectivamente); esto ocurrió en la Cumbre de Praga («beginning») planteándose como un entorno donde se trazaban una serie de amenazas; esta concepción fue seguida de la Cumbre de Bucarest donde se definió una política inicial en el ámbito de la ciberdefensa («founding»), seguida de la de Lisboa (donde se propuso centralizar la capacidad sobre este asunto: «centralising»). No fue hasta el año 2014, en la cumbre de Gales, donde se definió el ciberespacio como un «core task» de la defensa colectiva («enhancing»).

En la Cumbre de Varsovia en el año 2016 fue planteada la existencia de un nuevo dominio de las operaciones: es en este punto donde se plantea por primera vez la posibilidad de realizar operaciones

militares en este nuevo dominio («operating»), y al mismo tiempo en este momento temporal se efectúa la primera declaración conjunta entre la UE y la OTAN sobre el asunto.

Posteriormente en 2018, en Bruselas, se definió el marco de actuación SCEPVA (3), en donde se planteaba la integración de efectos en el ámbito del ciberespacio y de nuevo se efectúa otra declaración conjunta sobre el asunto entre la UE y la OTAN; es allí en donde, al mismo tiempo, se define una política de datos y una estrategia inicial sobre inteligencia artificial. Podríamos hablar del modelado, la adaptación a la situación concreta, o lo que en términos militares se suele definir como el «shaping» (una expresión en definitiva muy utilizada en el ámbito militar que en globa el conjunto de acciones encaminadas a definir y adecuar la preparación de las fuerzas propias y las acciones precursoras en el campo de batalla).

Por otra parte, y en relación con los objetivos planteados por la UE, hay que esperar hasta el año 2004, que es cuando se crea la ENISA (Agencia de la UE para la ciberseguridad), como núcleo inicial («beginning») de la concienciación de la importancia del ciberespacio a nivel europeo; sucesivamente en el año 2013 se vieron enumerados los objetivos («founding») en la primera así llamada «Estrategia Europea de Ciberseguridad: un Ciber-Espacio abierto y seguro»(4).

Sucesivamente, la «Estrategia Global para la Política Exterior y de Seguridad de la UE» de 2016 mantiene estos objetivos, además de poner el énfasis en la necesidad de «[…] *buscar el conseguimiento de sistemas innovadores para las tecnologías de información y comunicación (TIC), que garanticen la disponibilidad y la integridad de los datos*».

El 9 de agosto de 2017, entró en vigor (podemos estimar que nos encontramos en la parte de «centralising») la «Directiva del Parlamento Europeo y del Consejo relativa a medidas destinadas a garantizar un nivel común de seguridad de las redes y sistemas de información de la Unión» (la conocida como Directiva NIS). Esta normativa buscó mejorar la seguridad de los Estados miembros de la Unión Europea, que dispusieron hasta el 25 de mayo de 2018 para adaptar sus propias legislaciones a la nueva directiva. Sucesivamente entraría en vigor a finales de 2022 la Directiva NIS 2, que es la que desarrolla la anterior y está actualmente en vigor.

La publicación de la directiva NIS 2 (5) (incluida dentro del «enhancing») al eliminar las divergencias tan pronunciadas entre los Estados miembros en la aplicación de la directiva sobre la seguridad de las redes y sistemas de información —la mencionada Directiva NIS— de 2016, permitió la potenciación de la capacidad europea civil en el ciberespacio, concretamente mediante:

— La definición de normas mínimas relativas al funcionamiento de un marco regulador coordinado y,
— La actualización de la lista de sectores y actividades sujetos a las obligaciones de ciberseguridad (6).

En definitiva, la UE actualmente posee su propia ciberestrategia y política de seguridad en este dominio, donde, en diferentes documentos, se definen, particularmente, las posibles áreas de cooperación con la otra gran organización de seguridad atlántica: la OTAN.

Por ejemplo y en relación con el ciberespacio, se contempla por esta organización el establecimiento de «estándares» comunes relativos a la certificación de los sistemas de tecnologías de la información («Cyber Resilience Act»: CRA), una referencia para sistemas militares y no militares.

El «CRA», sería una acción correspondiente al hito definido como «operating», cuya aprobación oficial por la UE se espera ocurra en 2024, y tiene como principal misión cubrir los vacíos existentes en el código. Esto se realiza mediante la creación de una legislación horizontal que defina los estándares de ciberseguridad europeos (para productos y servicios digitales).

Además, finalmente y para la UE, es muy importante la actividad y sinergias que se puedan canalizar a través del Fondo Europeo de Defensa (7). Quedando también patente la importancia del intercambio de información en lo relativo a doctrina y planeamiento con sus socios (8); y la mejora del conocimiento de la situación a través del intercambio de información (particularmente) entre NCIR (9) y CERT (10) (y la cooperación en la gestión de posibles crisis futuras, entre otra serie de medidas).

Por último, en la reciente cumbre de Madrid (2022) se formuló una nueva declaración conjunta entre las dos organizaciones, seguida de una subsiguiente en 2023. Posteriormente analizaremos éstas.

PREMISAS BÁSICAS: LAS NECESIDADES O BASES DE LA COOPERACIÓN DE LAS ORGANIZACIONES

Una vez estudiadas la situación en las dos organizaciones (por separado), abordaremos la situación de la colaboración entre la OTAN y la UE. Es evidente, que la OTAN y la UE desempeñan funciones complementarias, coherentes, que se refuerzan mutuamente en el apoyo a la paz y la seguridad internacionales, y que poseen un conjunto combinado de destacables instrumentos políticos, económicos, civiles y militares.

Así pues, en estos momentos, los documentos básicos («founding») que definen actualmente el marco general de cooperación entre la OTAN y la UE (en el ámbito del ciberespacio) son la Brújula estratégica de la UE (2022) y Esquema del concepto estratégico de la OTAN (2022) que materializan una serie de principios de cooperación y promueven una asociación

estratégica reforzada, que contribuye también, supuestamente al menos, a reforzar la EDITB.

En la definición de necesidades de una y otra organización podemos encontrar amenazas, y también objetivos, en relación a la deseada primacía tecnológica y militar (11):

- *«La asociación estratégica OTAN y la UE se basa en nuestros valores compartidos; nuestra determinación de hacer frente a los desafíos comunes y nuestro compromiso inequívoco con promover y salvaguardar la paz, la libertad y la prosperidad en la zona euroatlántica».* (Declaración conjunta OTAN UE 2023).

- *«Las tecnologías emergentes y disruptivas [...] están alterando el carácter de conflicto, adquiriendo mayor importancia estratégica y convirtiéndose en escenarios clave de la competencia global. …El acceso al espacio y al ciberespacio son fundamentales para una disuasión eficaz y defensa».* (Concepto Estratégico OTAN 2022).

Para la OTAN, y también para la UE (12), sin duda después de la ilegal invasión de Ucrania, la Federación de Rusia es la amenaza más importante y directa para la seguridad de los aliados, y para la paz y la estabilidad en la zona euroatlántica (13).

La visión y estrategia militar sobre el ciberespacio de la OTAN como dominio de operaciones se define actualmente por una serie de documentos entre los que destacan ya mencionados de 2018 (definición como Dominio de Operaciones), y la formulación operativa de los procedimientos de actuación de la OTAN, recogida en documentos de alto nivel como:

- El denominado OTAN «Warfare Capstone Concept» (NWCC) 2021, un concepto base para la ejecución de operaciones militares, en general.

- La «Cyberdefense Comprehensive Policy» (2021) y «Action Plan» (Plan de Acción de 2022),

- Documentación de la que derivan el AJP (14) 3.20 (2020) y el «Cyber adaptation Plan» (Plan de Adaptación Ciber (2022),

- Plan de desarrollo de las Organizaciones del Ciberespacio del «Allied Command for transformation (ACT)»,

- Y el denominado Concepto de «operaciones multidominio» (a ser aprobado próximamente, véase esquema a continuación).

Para la OTAN, actualmente, los objetivos primordiales de su actuación son promover la colaboración y cooperación en el «ámbito ciber» a través del creado Centro de Operaciones del Ciberespacio (Cyber Operations Coordination Centre o CyOC):

- Proporcionando una referencia sobre los aspectos relativos al dominio del ciberespacio de «Mission Assurance» (esto es, en general, la resiliencia de las capacidades ciber).

- Facilitando una visión del ciberespacio persistente, centralizado y completo.

- Liderando la preparación, planificación, conducción y coordinación o ejecución de operaciones en el ciberespacio.

Por otro lado, para la UE, de acuerdo a la Brújula estratégica, y otros documentos, en cuanto a «partenariados», lo más reseñable es la cooperación existente entre la UE y la OTAN. A las cuarenta y dos medidas establecidas inicialmente por la Unión en 2016 (referidas en general al ámbito de seguridad), se le han añadido posteriormente diversas iniciativas por ejemplo en materia de lucha antiterrorista y la «movilidad militar».

En 2022 el Consejo determinó que los ámbitos de actuación para los próximos años en el ámbito del ciberespacio serían:

- La creación de una red de centros de operaciones de seguridad,

- La ejecución de medidas e instrumentos de la UE para las redes 5G,

- La necesidad de apoyar el desarrollo de un «cifrado sólido»,

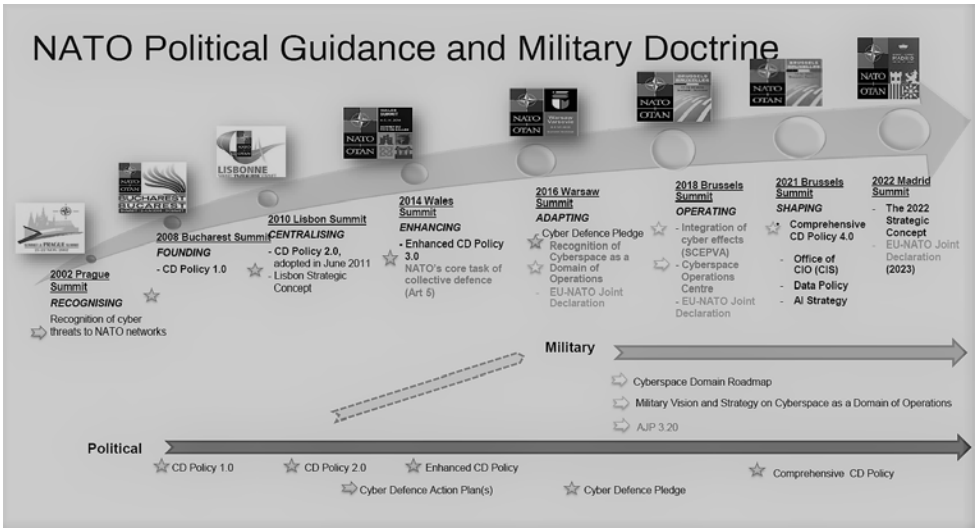
- La elaboración de una agenda para el desarrollo de la capacidad cibernética exterior de la UE al objeto de aumentar la ciber resiliencia y las ciber capacidades «en todo el mundo» (15).

Finalmente, en definitiva, la articulación de esta cooperación a nivel practico («centralising») se encuentra determinada, como se ha mencionado, en las Declaraciones de la UE de la OTAN sobre Cooperación de 2016, 2018 y particularmente la de 2023. En estas declaraciones se promueve la cooperación según los principios de apertura mutua, transparencia, complementariedad y respeto por los diferentes mandatos de las organizaciones, autonomía en la toma de decisiones e integridad institucional (16).

PRINCIPIOS Y OBJETIVOS DE COOPERACIÓN. CONCLUSIONES DERIVADAS DE LA DECLARACIÓN CONJUNTA UEOTAN DE 2023

El 10 de enero de 2023, la UE y la OTAN firmaron una Declaración conjunta en Bruselas. Este es un documento clave (junto con los periódicos informes de situación). Ambas condenaron la agresión de Rusia contra Ucrania y reiteraron su apoyo inquebrantable a este país. Particularmente, en esta declaración conjunta hubo una serie de referencias explicitas muy importantes relativas al ciberespacio; en ese sentido la UE y la OTAN se estima deberán ampliar e

GRÁFICO 1
EVOLUCIÓN POLÍTICA Y MILITAR DEL CIBERESPACIO



Fuente: CCD COE. Pernit Pirek.

intensificarán su cooperación en ámbitos como los de:

- Las tecnologías emergentes y disruptivas,
- La resiliencia y la protección de las infraestructuras críticas,
- El ámbito espacial,
- La manipulación de información e injerencia por parte de agentes extranjeros.

En concreto, en relación con la política y estrategia de ciberdefensa, y ahondando en el tema, sin ser explícita la mención de asuntos, sí que actualmente existen una serie de áreas concretas de cooperación (17) como:

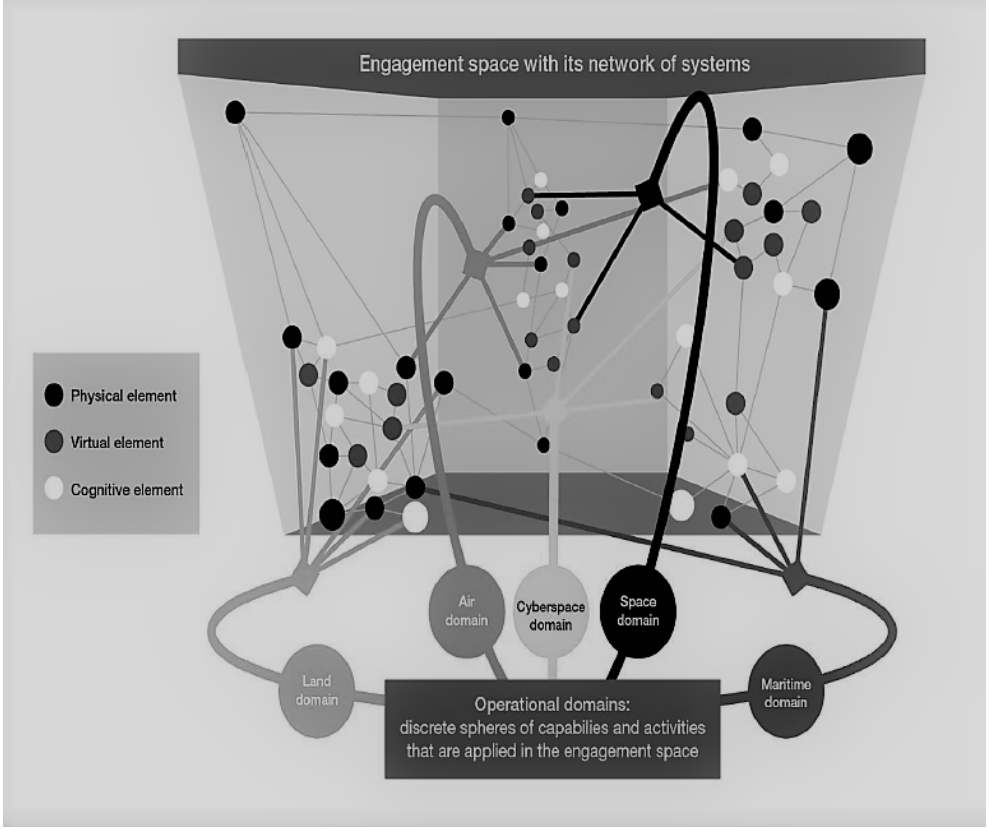
- Las Consultas políticas sobre el ciberespacio (tanto a nivel «staff» como reuniones de alto nivel),
- La coordinación entre el personal de ambas organizaciones en materia de ciber diplomacia pública,
- La contribución mutua a la «Situational awareness» o Conciencia situacional en el ciberespacio y la respuesta a crisis y desarrollo de capacidades con «partners» (incluyendo aliados, socios y cooperadores).
- La redacción y adopción de normas armonizadas y procesos de certificación similares (como los incluidos en el CRA).
- El fomento de la interoperabilidad de capacidades de intercambio de información en diferentes dominios (como por ejemplo a través de la NATO FMN).
- La participación por parte de la UE en el CCD-COE (18) de la OTAN,
- El establecimiento de un marco para la gestión y respuesta a crisis, el fomento de las actividades de educación, capacitación y ejercicios.
- Dentro de este marco general de cooperación se definen también nuevas iniciativas para fomentar el intercambio de inteligencia sobre amenazas cibernéticas e híbridas (a través del llamado «Working Group for Disinformation», que enlaza con el «Code of Practice on Disinformation 2022»).
- La realización de acciones incluidas en el Fondo Europeo de Defensa, Fondo de Apoyo a la Paz (19) y promovidas por el Consejo de la UE (en relación al Desarrollo de Capacidades Cibernéticas de la UE).

POSIBLES ÁREAS PARA «PROFUNDIZAR EN LA COOPERACIÓN 2023+»

Una vez analizado lo realizado hasta el momento, que es bastante como se puede comprobar, corresponde concluir con las posibilidades futuras de cooperación. Por parte de las dos organizaciones se contempla como un objetivo primordial la posible coordinación de posiciones comunes en el ámbito de la llamada ciber diplomacia y la ciberseguridad digital.

En este sentido se determina como un asunto muy relevante la coordinación de las acciones de «atribución de ataques» («attribution» en inglés) para identificar posibles agresores y así determinar posibles reacciones, que pueden acarrear acciones (incluidos en la llamada «Tool box» o Caja de herramientas de

ESQUEMA 1
ESQUEMA OPERACIONES MULTIDOMINIO. ACT (OTAN)



Fuente: OTAN.

la UE (20)) y que derivarían en, por ejemplo, sanciones colectivas o acciones individuales basadas en el derecho a la legitima defensa) en el ámbito de la diplomacia, que podrían involucrar, por ejemplo, incluso al Grupo de Expertos Gubernamentales y el GTCA (Grupo de trabajo de composición abierta) de las Naciones Unidas, y finalmente en la imposición de sanciones.

Esta «cyber diplomacy tool box» (2019) (21) fue concebida para poder realizar la atribución de ataques cibernéticos. Por ejemplo, el marco MITRE Att&CK (22) proporcionaría, en su caso, una descripción general de las evidencias técnicas y qué pistas pueden proporcionar sobre la autoría (23). Una vez identificado el autor procedería realizar la atribución y finalmente las acciones (una especie de «represalia», con matices…) que se estimen apropiadas.

En ese sentido, por ejemplo, en julio de 2020 por primera vez el Consejo de la UE decidió imponer medidas restrictivas contra 6 personas y 3 entidades responsables de diversos ciberataques (24).

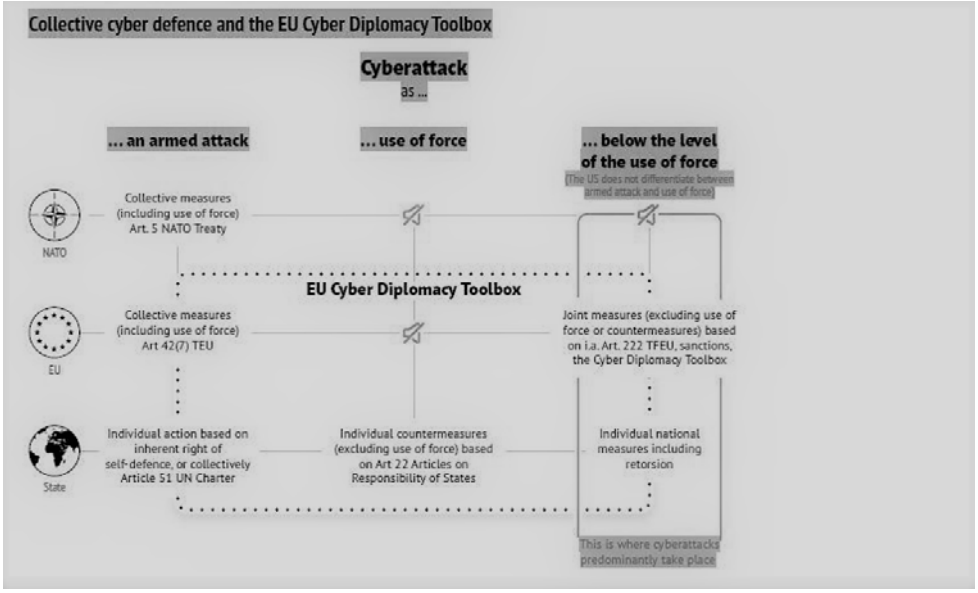
En Julio 2021 diversos aliados como Canadá, los Estados Unidos, atribuyeron la responsabilidad por el ataque al servidor de Microsoft Exchange a la República Popular China. En septiembre 2022 Albania sufrió un ciberataque que fue atribuido a Irán, y finalmente en mayo de 2022 se realizó por primera vez la atribución colectiva del Consejo de la UE / AR del ciberataque VIASAT/KA SAT (una red de satélites) a Rusia.

En este sentido, por parte de la OTAN y la UE, sin ser totalmente exhaustivo, se vislumbran como posibles las siguientes áreas de cooperación:

1) En los últimos años, la Alianza y la Unión han manifestado públicamente su interés en las EDT (25) y la necesidad de profundizar en su desarrollo e implantación. En la actualidad se han delimitado, de manera general, una serie de áreas prioritarias en el ámbito de ciencia y tecnología: Inteligencia artificial/Autonomía (Big Data, sensores; Tecnología cuántica (recopilación, procesamiento y explotación de datos); Tecnología de satélites (mayor potencia, menor tamaño); Tecnología espacial/Hipersónica.

2) En relación con todo lo anterior, se intuye la importancia de la diplomacia parlamentaria recíproca y se reiteran sus anteriores llamamientos en favor de un mayor papel de la Asamblea Parlamentaria de la OTAN y el Parlamento Europeo; reconociendo por ejemplo a la delega-

ESQUEMA 2
FUNCIONAMIENTO «EU CYBER DIPLOMACY TOOL BOX»



Fuente: UE.

ción del Parlamento Europeo en la Asamblea Parlamentaria de la OTAN la condición de miembro de pleno derecho, de modo que se refleje la importancia de la cooperación UE-OTAN;

3) Es evidente existe un interés común en desarrollar las capacidades de computación en la nube («cloud computing»), conocida también como «servicios en la nube», que no es sino el uso de una red de servidores remotos conectados para almacenar, administrar y procesar datos, servidores, bases de datos, redes y software. En lugar de depender de un servicio físico instalado, se tiene acceso a una estructura donde el software y el hardware están virtualmente integrados (26).

4) Existe un interés común en promover particularmente en Europa el despliegue de fibra y servicios basados en el 5G. En concreto, el conjunto de herramientas 'The Connectivity Toolbox' ha sido acordado por todos los Estados miembros de la UE, en colaboración con la Comisión Europea, para acelerar el despliegue de la fibra y el 5G en la UE.

5) Hay un interés de la OTAN en promover la actuación de la agencia DIANA (27) para promover la actuación de proveedores de «tecnología profunda y de doble uso» (2021).

6) Existe una directriz de alto nivel político en promover la participación de las naciones en el Fondo de Innovación de la OTAN (2022): lanzado por 21 países este es el primer fondo de capital riesgo multi-soberano del mundo, que, a través de las iniciativas como DIANA, promueve la participación de 100 centros de investigación y tiene un marco temporal de actuación a quince años vista.

7) Es necesario involucrar a capital riesgo multi empresarial para empresas emergentes. Se vislumbra que la cooperación publico privada, y del sector militar con otras áreas, mediante la promoción de tecnologías de doble uso, será uno de los aspectos a desarrollar en el futuro.

8) Es muy conveniente continuar desarrollando normas técnicas y de certificación conjuntamente (como el CRA).

9) Es muy beneficioso continuar promoviendo la Cooperación civil y militar en el ciberespacio (red CERT militar de la UE, participación conjunta en el foro de comandantes de mandos del ciberespacio y otras).

10) Se considera necesario mejorar la cooperación con la industria, el mundo académico y la sociedad civil: por ejemplo, la Iniciativa de Democracia Digital 2023 de y los programas de programa Europa Digital.

11) Además, finalmente, la UE ha solicitado igualmente que se celebre una reunión conjunta de la Comisión de AAEE del Parlamento Europeo y de la Cámara de Representantes de los Estados Unidos a fin de debatir sobre las amenazas comunes a la asociación transatlántica en materia de seguridad y sobre cómo podría ayudar a afrontarlas una mejor cooperación entre la Unión y la OTAN (28).

CONCLUSIÓN

En definitiva, y como conclusión, las relaciones en el ámbito del ciberespacio podrían contribuir a reforzar verdaderamente la base tecnológica europea, sin embargo, existe el peligro (evidente), no seamos incautos, que algunas de estas iniciativas promuevan la implantación en la UE de tecnológicas o industrias de defensa estadounidenses (Microsoft, Apple, Meta, Lockheed Martin,…), británicas (BT, Revolut, BAE,…) , e incluso canadienses, o turcas … a través de alianzas estratégicas y acciones a nivel regulatorio, diplomático y político, en detrimento de países y empresas de la UE…

No existe, sin embargo, otra alternativa que tratar de cooperar con la OTAN por diversos motivos (economías de escala, capacidades relativas a la investigación, I+D, cadenas de suministro y sobre todo la «competición» tecnológica con China, mecanismos de atribución …), al menos hasta el momento, por ello es necesario buscar las sinergias de esta colaboración OTAN-UE tratando de mantener la autonomía estratégica (EDITB) para contribuir al desarrollo tecnológico de las naciones de la UE y la constitución de una autentica capacidad civil y militar en un ámbito tan transcendental como el del ciberespacio en Europa (y nuestros aliados recíprocamente…).

La clave estaría en cómo llevar a cabo este proceso salvaguardando al mismo tiempo los intereses políticos, comerciales, industriales y militares de la UE: sin duda una prioridad para la actual agenda estratégica de la UE.

NOTAS

[1] Utilizaré los términos en ingles porque todos los estudios y referencias sobre el tema se tratan en esta lengua (Nota del autor).

[2] «Comenzando, fundando, centralizando, promoviendo, operando y adecuando y ajustando».

[3] SCEPVA: Sovereign Cyber Effects Provided Voluntarily by Allies. Del inglés. Efectos Ciber Soberanos proporcionados voluntariamente por los Aliados.

[4] Comisión Europea, 2013, 4-14.

[5] DIRECTIVA (UE) 2022/2555 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) n. 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2).

[6] DSN, Gobierno de España, Presidencia del Gobierno (2023), https://www.dsn.gob.es/es/actualidad/sala-prensa/publicaci%C3%B3n-directiva-nis2

[7] El Programa de Trabajo 2023 del Fondo Europeo de Defensa proporcionará 1.200 millones de euros para investigación e innovación en materia de defensa a través de sus convocatorias anuales de propuestas.

[8] Como por ejemplo participando en el desarrollo de la NATO FMN: «Federated mission network», una red de redes de la OTAN que permitirá la interoperabilidad entre los aliados, que podrán acceder a determinados dominios de la información, o redes de misión en función de las necesidades operativas.

[9] NATO Computer Incident Response Capability (NICRC). Nace en 2019 con el objetivo de llevar a cabo de manera segura la conducción de operaciones y misiones. No olvidemos que se compone de una comunidad superior a los 100.000 usuarios en más de 50 puntos de acceso. Por poner un ejemplo, que da idea de la magnitud de la entidad, el NCSC (NATO Cyber Security Centre) analiza y guarda más de 20TB (terabytes) de información al día. GARCIA SERVENT y IGLESIAS POSADA (2020), De a ciberdefensa en el ámbito de la OTAN. ¿Un problema de concepto?, www.elradar.es

[10] CERT -UE. Computer Incident Response Team. El CERT-EU está formado por un equipo de expertos en seguridad informática de las instituciones y los órganos de la UE. Recopila, gestiona, analiza y comparte información sobre amenazas, vulnerabilidades e incidentes relacionados con infraestructuras TIC no clasificadas.

[11] PERNIT PIREK (2023), Cyberspace Strategic Outlook 2030: Horizon Scanning and Analysis, CCD COE NATO.

[12] Durante el Consejo Europeo del 23 de junio de 2022, los dirigentes de la UE concedieron a Ucrania el estatuto de país candidato a la adhesión a la UE.

[13] Es patente que, para la OTAN, del mismo modo: «». Las operaciones híbridas y cibernéticas maliciosas de la República Popular China y su retórica de confrontación y desinformación atacar a los aliados y dañar la seguridad de la Alianza. La República Popular China busca controlar tecnologías e industrias clave, sectores, infraestructura crítica y materiales estratégicos y cadenas de suministro… (Concepto Estratégico 2022).

[14] AJP: Allied Joint Publication.

[15] Consejo de la UE (2020), Ciberseguridad: Adopta unas Conclusiones sobre la Estrategia de Ciberseguridad de la UE.

[16] Declaración de la Cumbre de Madrid (2022).

[17] Véanse informes de situación periódicos de la UE (Nota del autor).

[18] CCD COE: Cyber Defense NATO Cooperative Center of Excellence.

[19] El Fondo Europeo de Apoyo a la Paz es un instrumento extrapresupuestario destinado a reforzar la capacidad de la Unión de: prevenir conflictos, consolidar la paz y reforzar la seguridad internacional. Se puso en marcha en 2021 y reemplaza y amplía el mecanismo Athena y el Fondo de Apoyo a la Paz para África.

[20] La primera versión de una «caja de herramientas» común de la UE para así aplicar la «cartera de identidad digital» de la UE fue publicada el 10 de febrero de 2023.

[21] Decisión del Consejo (UE), 2019-796 y 797, https://www.cyber-diplomacy-Ctoolbox.com/#:~:text=%2D%20Council%20Decision,2019/796.

[22] MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT & CK).
[23] MATABIT TELLECHEA P. (2019), CIEEE, «Atribución en el ciberespacio». p. 7 y ss.
[24] Entre los que se encontraban los responsables del intento de ciberataque contra la OPAQ (Organización para la Prohibición de las Armas Químicas) y los ampliamente conocidos WannaCry, NotPetya y Operation Cloud Hopper.
[25] EDT: Emerging and disruptive technologies. Tecnologías disruptivas y emergentes.
[26] SCHMIDT C. (2023), Governance & Cyber -Threats to Democracy, Cybersecurity Trends. Tartu University (Estonia).
[27] «Defense Innovation Accelerator for the North Atlantic». En 2021 la Alianza Atlántica acordó impulsar el lanzamiento de un «acelerador de innovación» que recibió el nombre de DIANA (Aceleradora de Innovación en Defensa para el Atlántico Norte). En abril del año pasado los ministros de Asuntos Exteriores de los países de la OTAN aprobaron los estatutos de DIANA. En Madrid se firmó la carta de compromiso con el Fondo de Innovación de la Alianza, que contará con 1.000 millones de euros para programas.
[28] Resolución del Parlamento Europeo, de 7 de julio de 2021, sobre la cooperación UE-OTAN en el contexto de las relaciones transatlánticas (2020/2257(INI)).