Una idea para potenciar la capacidad de disuasión de la OTAN en el ciberespacio

Enrique Cubeiro Cabello
Capitán de navío, Reserva

La utilización del ciberespacio como nuevo ámbito de las operaciones militares plantea numerosas retos para el ejercicio de la disuasión y, muy especialmente, para la disuasión por represalia. El ciberespacio juega un papel cada vez más importante en el devenir de los conflictos, se adivina entorno decisivo en los conflictos venideros y son muchos los Estados que cuentan ya con potentes capacidades ofensivas para operar en este nuevo campo de batalla. La OTAN ha tardado en reaccionar y entra en esta parti-da con mucho retraso y diferentes reglas, más restrictivas, que sus potenciales adversarios. La actual aproximación de la Alianza a la obtención e integración de capacidades ciberofensivas en las operaciones parece de difícil aplicación, por lo que es preciso contemplar nuevas alternativas para la integración de estas capacidades. Solo así, la Alianza podrá alcanzar cierta capacidad de disuasión y alguna posibilidad de control del ciberespacio en caso de conflicto

Disuasión

El diccionario de la RAE define disuasión como "la acción y efecto de inducir o mover a alguien, con razones, a cambiar de opinión o a desistir de un propósito". Requiere, por tanto, de la existencia de dos voluntades antagónicas o, al menos, divergentes en la intención.

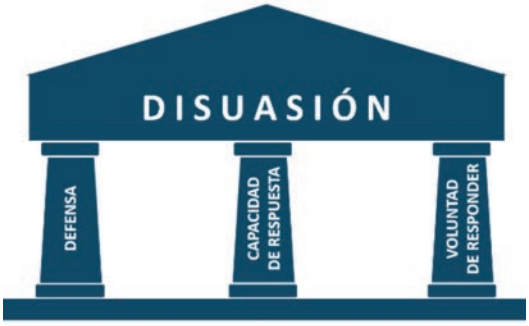
La disuasión es elemento fundamental en cualquier modelo de seguridad y, desde hace siglos, uno de los instrumentos a disposición de los Estados para ejercitar su poder. Ejercicio que se lleva a cabo por medio de dos modelos generalmente complementarios: el de negación y el de represalia.

En el primero, el potencial atacante ha de percibir una enorme dificultad en alcanzar sus objetivos. Dificultad que puede provenir de un

elevado coste (económico o en vidas humanas), de la gran dificultad técnica que requiere llevar a cabo la acción y, en algunos casos en los que el sigilo o el anonimato sean decisivos, de la posibilidad de ser detectado o identificado.

La disuasión por represalia se fundamenta en el temor a las acciones que pueda llevar a cabo la víctima como respuesta al ataque o al intento de llevarlo a cabo.

De lo anterior, se deduce que la disuasión se sustenta en tres pilares. Por una parte, una sólida defensa, que fundamenta la disuasión por negación. Y, por otra, de una capacidad de respuesta acompañada de la voluntad de utilizarla contra un eventual atacante, que fundamentan la disuasión por represalia.



La disuasión es en buena medida una declaración de intenciones. Pero solo tendrá consistencia si el mensaje que se lanza al exterior goza de credibilidad. Credibilidad cuyo primer sustento, obviamente, está en poseer (o hacer creer que se poseen) las capacidades técnico-operativas que permitan tanto la defensa como la respuesta.

Pero el elemento decisivo de la credibilidad es la voluntad manifiesta y real de defenderse. Es decir, que el potencial agresor perciba en su potencial víctima una firme intención de que va a emplear la fuerza en el caso de que sea atacado.

CIBERDISUASIÓN[1] VERSUS DISUASIÓN NUCLEAR

Podríamos definir "ciberdisuasión" como la disuasión que se ejerce en o a través del ciberespacio.

(1) A lo largo de este artículo se emplea el prefijo "ciber" como sinónimo de "ciberespacial", "del ciberespacio" o "en el ciberespacio".

La escasa experiencia real en ciberguerra[2] hace que casi todo lo relativo a ella se mueva todavía en el terreno de la especulación. Uno de esos aspectos que aún resulta muy opaco es la forma en la que las capacidades de ciberdefensa, especialmente las ofensivas, pueden modificar la naturaleza de los conflictos venideros. Y, para argumentar posturas e ideas y tratar de llenar esas lagunas de conocimiento, con mucha frecuencia se recurre a modelos conocidos.

Así, por ejemplo, desde que el ciberespacio se convirtió de forma clara en un nuevo campo de batalla (y en un nuevo ámbito de las operaciones militares), son muchos los analistas que han alertado sobre la altísima posibilidad de un "Ciber-Hiroshima" o un "Ciber-Pearl Harbour", y hasta se han acuñado expresiones como "la destrucción mutua asegurada en el ciberespacio". De ahí que exista una fuerte tendencia a plantear un nuevo modelo de orden mundial basado en la ciberdisuasión, buscando similitudes con el sostenido en la etapa de la Guerra Fría por medio de la disuasión nuclear.

¿Pero existe realmente ese paralelismo? Analicémoslo.

La Figura 1 muestra el denominado vórtice de escalada del conflicto bélico. Sobre él, se representan los rangos de intensidad de las diferentes acciones que pueden desarrollarse mediante los diferentes tipos de guerra. Una mayor intensidad implica un mayor efecto sobre el adversario.

Los vectores representan los márgenes de intensidad de los distintos tipos de capacidades militares. Como podemos ver, las intensidades máximas corresponden a las capacidades nucleares. Las capacidades convencionales permiten rangos de intensidad de los efectos que varía entre mínimo y muy alto, correspondiendo este último a ataques convencionales masivos.

En cuanto a las capacidades ciber, permiten llevar a cabo acciones de intensidad mínima (ciber ISR[3] sobre la infraestructura del adversario, ciberataques de escasos efectos), pero también acciones de muy elevada intensidad en cuanto a sus efectos (por ejemplo, ciberataques masivos contra infraestructuras críticas y servicios esenciales), por encima incluso de las que pueden obtenerse mediante ataques masivos convencionales. Este inusual margen de gradación

---

(2) Posibles definiciones: a) conflicto armado que se desarrolla fundamentalmente en o a través del ciberespacio"; b) acciones bélicas que tienen lugar en el ciberespacio, como entorno separado o como parte de una operación multidominio".

(3) Intelligence, Surveillance & Reconnaissance.

de la ciberguerra pone a disposición del comandante, al menos en teoría, un abanico de acciones y efectos asociados que no existe en los otros tipos de guerra. Podemos decir que combina las posibilidades de gradación de la guerra convencional con unos máximos de intensidad similares a los alcanzables mediante medios nucleares (y sin muchos de sus indeseables y perdurables efectos colaterales).

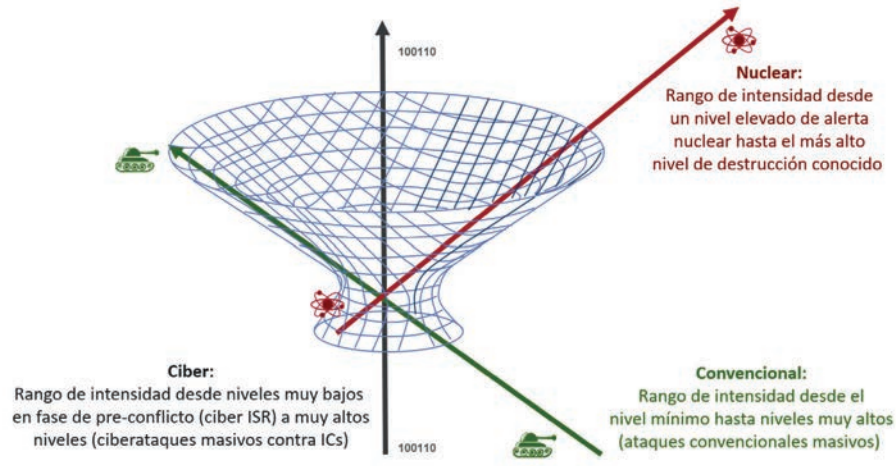


Figura 1 – Comparativa de los rangos de efectos entre las capacidades convencionales, nucleares y ciber.

De lo anterior, podemos inferir la existencia de, al menos, una similitud fundamental entre la ciberdisuasión y la disuasión nuclear: ese rango de intensidad máxima que genera la posibilidad de que dos grandes Estados en conflicto puedan infringirse enormes daños.

Y otro más, muy evidente: que ambos tipos de capacidades posibilitan lo anterior sin desplazar grandes fuerzas ni ocupar el territorio del adversario.

Sin embargo, si analizamos más a fondo las características de la guerra nuclear y la ciberguerra, veremos que aquí acaban sus similitudes.

Volviendo de nuevo al vórtice, mientras la guerra nuclear se manifiesta poco menos que en dos únicos estados: "on" y "off", teniendo cualquier estado "on" enormes efectos, la ciberguerra permite llevar a cabo acciones de intensidad muy diversa.

Existen también grandes diferencias en lo relativo a la actividad, muy intensa en todo momento en el ciberespacio, independientemente de que hablemos de tiempo de paz, crisis o conflicto, mientras que resulta prácticamente nula en el plano nuclear (como es bien sabido, desde Nagasaki 1945 el armamento nuclear no se ha vuelto a utilizar en conflicto alguno) y quedaría circunscrita a aspectos tales como despliegues o ensayos.

Otras diferencias importantes se encuentran en lo referente al número y calidad de los actores (muy escasos, perfectamente identificados y exclusivamente en forma de Estados en lo referente a la guerra nuclear, y numerosísimos, enormemente variados y completamente dispersos en el ciberespacio, incluyendo infinidad de actores no estatales) y el armamento (muy reducido y controlado en el ámbito nuclear y extraordinariamente numeroso, disperso, accesible a muchos y sin posibilidad de control alguno en el ámbito ciberespacial).

Otra notable diferencia es que todo lo que rodea a la actividad nuclear es relativamente fácil de observar e interpretar (preparativos, niveles de alistamiento, efectos); sin embargo, por muy diferentes motivos que se tratarán más adelante, en el ciberespacio todo resulta muy opaco y confuso.

Mientras la guerra nuclear se sustenta en la simetría, la ciberguerra es el paradigma de la guerra asimétrica: un pequeño grupo atacante sin demasiados recursos económicos puede causar graves daños a un Estado poderoso. No hay ningún armamento comparable a una ciberarma en términos de eficacia coste. Esto, a su vez, posibilita la disuasión del débil al fuerte.

En el ámbito nuclear, la disuasión se genera con la mera posesión de las armas y sus medios de lanzamiento. En el ciberespacio, como veremos, esto no es así.

Del somero análisis anterior, resulta evidente que las diferencias son muchas y sustanciales y podemos extraer dos primeras conclusiones:

- Que la ciberguerra permite efectos sobre el adversario comparables a los que se podrían obtener mediante medios nucleares y con una posibilidad de gradación similar a la que proporcionan los medios convencionales.
- Que, de existir un modelo de disuasión en el ciberespacio, éste ha de construirse a partir de unos fundamentos completamente diferentes a los del modelo nuclear.

Dificultades para la disuasión en el ciberespacio

La naturaleza singular del ciberespacio presenta muchas y serias dificultades para el ejercicio de la disuasión en y a través de él.

Una de las principales es la complejidad de la defensa, que además se acrecienta cada día como consecuencia del crecimiento próximo a lo exponencial de las amenazas, pero sobre todo de la superficie a defender y de las vulnerabilidades asociadas a los elementos interconectados.

Los dispositivos conectados a Internet se cuentan ya por decenas de miles de millones. Cada dos años se producen y almacenan tantos datos como en toda la Historia anterior de la Humanidad. Existe ya una total ciberdependencia, que afecta a empresas, organizaciones, ciudadanos y a todos los sectores de actividad. Y todo ello se hará aún más complejo de gestionar a medida que eclosionen nuevas tecnologías que incrementen el empleo de los datos y estimulen la conectividad, como el Big Data, la Inteligencia Artificial, la computación cuántica o el 5G. Esta situación ha difuminado el perímetro a defender, hasta el punto de que la mayoría de las organizaciones y empresas desconocen dónde empiezan y acaban sus activos en el ciberespacio.

Y mientras todo esto ocurre, la creación de un malware continua requiriendo como promedio unas decenas de líneas de código, en tanto el software de seguridad necesita ya de millones de líneas.

Todo ello se traduce en una situación en la que los atacantes van siempre por delante de los defensores en un ámbito en el que la tecnología avanza de forma extraordinariamente rápida, muchísimo mayor que en el resto de dominios en los que se ejecutan las operaciones militares.

Tampoco contribuye a robustecer la ciberdisuasión el que exista un convencimiento universal de que el ciberespacio es una especie de universo paralelo que se rige por sus propias reglas y que nada tiene que ver con el mundo real. Según esa visión, en el ciberespacio aplicaría algo semejante a ese "lo que ocurre en Las Vegas queda en Las Vegas". El hecho de que, por motivos diversos, no se de publicidad a los ciberataques sufridos y el que la gran mayoría queden impunes contribuye a sustentar esa imagen distorsionada del ciberespacio como "territorio sin ley" y ejerce un fuerte efecto llamada.

Y si en el resto de los dominios de la guerra la mayor parte del armamento está en poder de los Estados y el ejercicio de la fuerza

prácticamente limitado a unas fuerzas armadas sometidas a los poderes políticos, en el ciberespacio hay infinidad de armas al alcance de cualquiera, sin que exista ningún tipo de control (que sería, en cualquier caso, imposible de ejercer) y, además, sin los condicionantes de espacio-tiempo que limitan la posibilidad de actuar en los dominios convencionales.

Por otra parte, una misma acción en el ciberespacio puede ser categorizada como ciberdelito, ciberterrorismo o ciberguerra en función de las circunstancias que la rodean; entre ellas, por la condición del atacante y del atacado y por el acto en sí, pero, fundamentalmente, por su motivación. Un acto de ciberdelito no debería ser respondido con otro de ciberguerra, por lo que la determinación de la autoría de un ataque y su motivación resultan fundamentales a la hora de ejercer una respuesta. Y lograr esto es extraordinariamente complicado.

Además, mientras en el mundo real la actividad bélica está muy limitada a los conflictos en curso, y estos no son demasiados y es posible seguir su evolución, en el ciberespacio existe una frenética y permanente actividad hostil. Podríamos hablar incluso de una guerra soterrada, que en la mayoría de los casos se realiza de forma sigilosa, en la que participa ese ecosistema de ciberamenazas tan heterogéneo en lo referente a capacidades como a motivaciones.

Existen infinidad de técnicas para dificultar la trazabilidad de un ataque. El anonimato es algo relativamente sencillo de conseguir en el ciberespacio, incluso con escasos recursos económicos. También resulta muy fácil la suplantación de identidad y la utilización de infraestructuras y medios de terceros, lo que propicia los ataques de bandera falsa, cada vez más habituales. Todo ello complica, y muchas veces imposibilita, tanto la trazabilidad del ataque como su consiguiente atribución. Y si se desconoce la identidad del agresor, difícilmente se le podrá responder.

Se habla mucho de la tremenda dificultad de perseguir eficazmente el ciberdelito, debido, entre otros muchos aspectos, a su habitual carácter transnacional, a la infinidad de zonas grises en los códigos penales y a la falta de una homogeneidad universal entre estos, a la profunda carencia de recursos especializados y a lo complejo de obtener evidencias probatorias. Pero es en su traslación al derecho de los conflictos armados dónde la indefinición legal del ciberespacio alcanza su máxima expresión: ¿Qué es un ataque armado en el ciberespacio? ¿O un acto hostil? ¿Cuándo es legítimo el uso de la fuerza en respuesta a una agresión?

La única aproximación seria a este problema ha sido el Manual de Tallin en sus dos volúmenes[4]. Pero no dejan de ser otra cosa que el trabajo de un grupo de expertos, sin ningún efecto vinculante. Y que, además, son objeto de fuertes controversias. Por lo tanto, podemos decir que existe un general consenso en aceptar que el Derecho Internacional de los Conflictos Armados aplica en el ciberespacio, pero que existen grandes discrepancias en el cómo.

Ante esa indefinición, resulta muy difícil establecer incluso algo tan esencial para la disuasión por represalia como es el umbral que dispara el derecho a la legítima defensa. Por otra parte, la definición de esa línea roja constituye en sí misma una debilidad, pues implícitamente se estará declarando que no existirá represalia para todo aquel ataque por debajo de ese umbral.

Además, la dificultad de determinar la autoría de un ciberataque implica que puede transcurrir un tiempo considerable (semanas, meses) entre el momento en el que se produce la agresión y aquel en el que se está en condiciones de acometer la represalia, lo que contraviene uno de los condicionantes para la aplicación del principio de legítima defensa, que es el de la continuidad temporal entre la agresión sufrida y la respuesta. Esto, por lo general, obligará al Estado agredido a emplear formas de réplica diferentes a la fuerza militar (protestas diplomáticas, sanciones, etc.).

Otro factor que complica tanto la defensa como las acciones de respuesta es el hecho de que más del noventa por ciento de las infraestructuras TIC existentes en el mundo están en poder de compañías privadas. A lo anterior se suma la creciente interconexión entre sistemas. Por tal motivo, resulta muy complicado que una acción en el ciberespacio contra un actor concreto no repercuta en terceros. Esto es de especial importancia al considerar acciones de represalia. Hoy en día, en toda acción militar se tienen muy en cuenta los posibles daños colaterales y existen procedimientos y herramientas que permiten predecir con notable precisión estos efectos asociados a los diferentes tipos de armamento convencional contra un objetivo concreto. En el ciberespacio, esos efectos no son nada fáciles de predecir, en tanto las interconexiones entre sistemas pueden llevar a una propagación en cascada que puede afectar muy seriamente a infraestructuras y servicios muy distintos del objetivo militar perseguido. Para determinados gobiernos, esta sola circunstancia puede suponer una luz roja en permanencia para el empleo de ciberataques en represalia.

---

(4) Tallinn Manual on the International Law Applicable to Cyber Operations (2013) y Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2017).

Además, para que la disuasión por represalia funcione, la capacidad de mostrar la fuerza es crucial. Esa demostración fue necesaria incluso para el arma nuclear. Pero esto no es igual para las ciberarmas. Los ciberataques son posibles porque existen vulnerabilidades en los sistemas objetivo. Una demostración de poder en el ciberespacio implica alertar al adversario de la existencia de la vulnerabilidad que se explota. Ello da lugar a que las ciberarmas sean difícilmente reutilizables pasado un cierto tiempo, ya que cualquier uso revelará información que puede servir al adversario para defenderse contra ataques futuros. Por tal motivo, hay que evaluar muy cuidadosamente su empleo.

Pero hay más condicionantes

El árbol de decisión que muestra la figura 2 corresponde, con ligeras modificaciones, al estadounidense Martin C. Libicki, autor de algunas de las obras más interesantes y visionarias que se han escrito sobre ciberguerra y ciberdisuasión. Como puede verse, las condiciones que Libicki considera que deberían de cumplirse antes de aventurarse a lanzar un ataque de represalia en el ciberespacio pasan por tener certeza razonable de que el ataque recibido proviene de un Estado, que sus efectos hayan sido públicos, que pueda ser atribuido a un Estado concreto – sin posibilidad de error y, además, de forma rápida -, que se disponga de una forma para ejercer la represalia, que puedan ser controlados los efectos de esa acción sobre terceros, que la contra-represalia sea poco probable,…

Demasiadas condiciones

Desde hace años, el Ciberespacio juega un papel fundamental en las estrategias híbridas, entendidas como aquellas que hacen uso coordinado y sincronizado de todas las capacidades disponibles para erosionar al adversario, a ser posible sin sobrepasar el umbral que podría desencadenar una repuesta militar. Especialmente, a través de tres ejes de actuación, muy diferentes pero complementarios: ciberataques, desinformación y propaganda, explotando todas las singularidades del ciberespacio: ubicuidad, generalización, facilidades para la difusión, anonimato,… y, muy especialmente, las áreas grises de la legislación.

Ante las áreas grises, hay dos aproximaciones completamente diferentes: si no está claro que esté permitido, no lo hago; si no está claro que esté prohibido, lo hago. Y, para los que eligen esta segunda línea, si además es prácticamente imposible que se pueda probar la

autoría, el círculo está cerrado. Esta situación, que algunos autores ya han definido como *"asymmetrical lawfare"*[5] coloca en una clara posición de desventaja a las democracias occidentales (y, por extensión, a la OTAN y la UE) frente a aquellos Estados en los que la acción de los gobiernos no está sometida al escrutinio de la opinión pública ni al del resto de contrapoderes.

Ante este escenario, en el seno de la Alianza se observa, especialmente en los Estados de corte anglosajón, una tendencia a emplear un tipo de atribución que se conoce como "atribución política", y, a ser posible, de forma colectiva. Es decir, proceder a la acusación y señalamiento público cuando se tenga una certeza razonable de que la autoría de un ataque corresponde a un determinado Estado, aunque se carezcan de suficientes evidencias técnicas probatorias. No obstante, muchos Estados aliados se resisten a la aplicación de este modelo.

Podemos concluir, por tanto, que ni la disuasión por negación ni la disuasión por represalia funcionan todavía bien en el ciberespacio. Y, derivado de ello, que alcanzar una sólida capacidad de disuasión en el ciberespacio es, a día de hoy, algo prácticamente utópico.

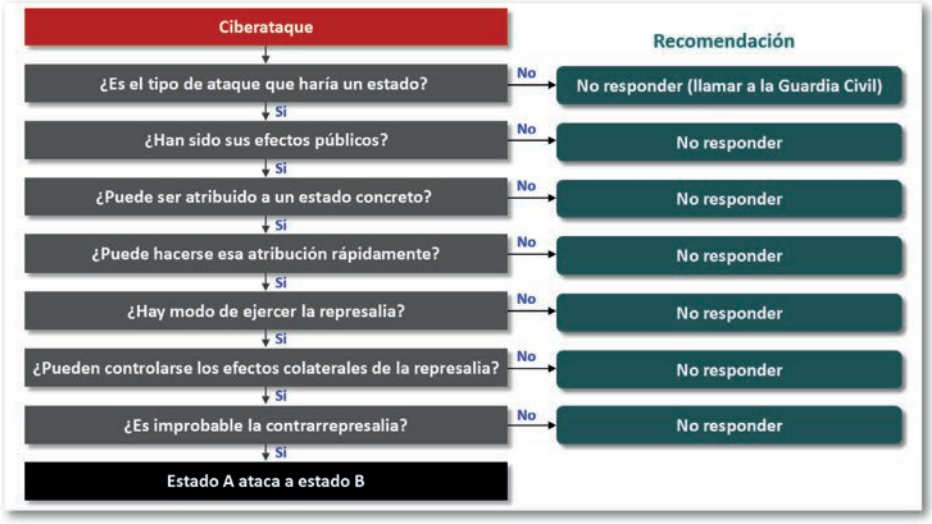


Figura 2 — Árbol de decisión para la ciber-represalia.

(5) SCHMITT, Michael N. Grey Zones in the International Law of Cyberspace. (2017).

Resulta evidente que construir una disuasión efectiva en el ciberespacio requiere un enfoque multidisciplinar que abarque, entre otros aspectos, la potenciación de la resiliencia y de las capacidades de defensa, trazabilidad y atribución, así como el reforzamiento legal, el control del ciberarmamento y la cooperación. Se trata, pues, de una tarea ardua y compleja, que involucra a un gran número de organizaciones y que, en muchos casos, dependerá de la voluntad y compromiso de los Estados. Lo cual no anima a ser optimista, habida cuenta de la existencia de unos bloques de poder con posturas y visiones muy encontradas de cómo ha de ser la gobernanza del ciberespacio y del marco legislativo y normativo que sobre él ha de aplicar.

Por lo tanto, podemos anticipar que las cosas van a seguir en la misma línea (de continuo empeoramiento) durante bastantes años.

Las capacidades ciberofensivas en las operaciones

Llegados a este punto, es necesario aclarar que una acción de represalia en legítima defensa no ha de producirse en el mismo dominio de las operaciones militares en el que se produjo la agresión. Así, al igual que una acción naval hostil puede ser respondida mediante un ataque aéreo (siempre que se ajuste a los principios que establece el Derecho Internacional de Los Conflictos Armados: oportunidad, proporcionalidad, etc.), un acto hostil en cualquiera de los ámbitos convencionales puede ser respondido con un ciberataque y viceversa, en lo que se conoce respuesta en dominios cruzados.

En cualquier caso, ha de advertirse que el empleo de una capacidad ciberofensiva no tiene porqué circunscribirse a la respuesta en legítima defensa, sino que será una capacidad fundamental en el caso de un conflicto armado que puede ser deliberadamente empleada contra un objetivo de interés.

También es importante entender que, al igual que ocurre en el resto de ámbitos de las operaciones, el objetivo de las fuerzas ciberespaciales es el de garantizar el libre uso del ciberespacio a las fuerzas propias y dificultárselo o impedírselo al adversario.

Sobre esa premisa, podemos distinguir cinco niveles de control del ciberespacio: cibersupremacía, cibersuperioridad, ciberparidad, ciberdegradación y ciberincapacidad:

- La cibersupremacía se alcanza cuando se tiene control absoluto del ciberespacio de confrontación. La libertad de acción propia es total mientras que la del adversario es mínima.

- La cibersuperioridad se alcanza cuando se dispone de una posición más favorable que la del adversario en el ciberespacio de confrontación, por lo que la libertad de acción propia es mayor que la de las fuerzas oponentes.
- La ciberparidad se produce cuando las fuerzas en conflicto disponen en el ciberespacio de similar libertad de acción y capacidad de interferencia sobre el adversario.
- La ciberdegradación se produce cuando el adversario está en una posición más favorable en el ciberespacio de confrontación, por lo que la libertad de acción propia es menor que la del adversario. La fuerza propia puede seguir operando en el ciberespacio, pero en modo degradado.
- La ciberincapacidad implica que el adversario tiene control absoluto del ciberespacio de confrontación, por lo que la libertad de acción propia es mínima mientras que la del adversario es total.

Obviamente, alcanzar la supremacía o la superioridad en el ciberespacio requiere disponer de capacidades defensivas y ofensivas. Contando exclusivamente con capacidades defensivas se podrá aspirar, a lo sumo, a la ciberparidad (y solamente cuando la ciberfuerza contraria tampoco disponga de capacidades ofensivas; en caso contrario, se estará condenado a la ciberdegradación o ciberincapacidad).

Y no se puede olvidar la transversalidad del ciberespacio. En realidad, su naturaleza es la de un "supra espacio", con enorme presencia e influencia en el resto de ámbitos. Esta transversalidad da lugar a que lo que ocurre en el ciberespacio repercuta intensamente en los otros ámbitos operacionales. Hasta el punto de que la superioridad del enemigo en este ámbito puede poner en riesgo la superioridad o supremacía propia en otros ámbitos, a pesar de que se cuente en ellos con mayores medios y capacidades que el adversario. Y esto es algo que cuesta hacer entender. Las operaciones terrestres, navales y aéreas se sustentan en sensores, sistemas de mando y control, de ISR, de combate, de armas,… todos ellos vulnerables a las ciberamenazas. Por tal motivo, el ciberespacio debe ser considerado de manera especial en todos los aspectos conjuntos (doctrina, planeamiento y conducción de las operaciones, orgánica, etc.)

La OTAN frente al ciberespacio

A mi juicio, durante muchos años la actitud de la OTAN frente al ciberespacio ha sido muy vaga y falta de orientación.

A ello han contribuido factores muy diversos, algunos ya mencionados, entre los que destaca la existencia entre sus miembros de posiciones muy distintas y, en algún caso, antagónicas respecto a las operaciones militares en el ciberespacio. También influyen las muy dispares capacidades de unos y otros, así como la enorme reticencia a compartir información relativa a este campo. Ello ha llevado a una situación en la que cada Estado ha hecho la guerra por su cuenta, paradójicamente en el dominio en el que resulta más evidente la existencia de una amenaza más activa, seria y, sobre todo, compartida.

Así, a pesar de la evidencia clara de que el ciberespacio se había convertido en un nuevo campo para las operaciones militares y de que las Fuerzas Armadas de un gran número de Estados acometían los necesarios cambios doctrinales y organizativos para dotarlas de medios y capacidades para operar militarmente en el ciberespacio, hay que esperar hasta 2016[6] (Cumbre de Varsovia) para que la organización reconozca al ciberespacio como "un dominio de operaciones en el que la OTAN debe defenderse tan efectivamente como lo hace en el aire, en tierra y en el mar" y se declare que la ciberdefensa estará integrada en la planificación operativa y las operaciones y misiones de la Alianza y apoyará la disuasión y defensa más amplias de la OTAN.

A pesar de esta declaración, los cambios organizativos y doctrinales desde entonces han sido escasos y se han producido con gran lentitud[7]. Así, por ejemplo, hasta principios del año 2020 no ve la luz el AJP 3.20 *Allied Joint Doctrine for Cyberspace Operations*, publicación que se limita a establecer unos principios muy básicos y que resulta de escasa utilidad práctica. Además, durante mucho tiempo, la mayor parte de las iniciativas de la Organización relacionadas con este campo se han enfocado a la defensa y lo que se ha dado en llamar "ciberdiplomacia", teniendo las operaciones ciberofensivas una consideración casi de asunto tabú.

Sin embargo, ante el escenario expuesto en los apartados anteriores, su más que probable evolución y el hecho constatado de que algunos de los Estados que más están apostando por alcanzar una mayor capacidad ofensiva en el ciberespacio y que mayor empleo están haciendo de las estrategias híbridas son China, Rusia, Irán o Corea

---

(6) Esa condición estaba reconocida en el Concepto de Ciberdefensa del JEMAD del año 2011. El Mando Conjunto de Ciberdefensa se crea en el año 2013.

(7) La relación de los principales hitos OTAN asociados a ciberdefensa puede encontrarse en: https://www.nato.int/cps/en/natohq/topics_78170.htm

del Norte, la OTAN se ha visto obligada a explorar alguna forma de integrar las capacidades ciberofensivas como elemento fundamental tanto para alcanzar un cierto grado de disuasión por represalia como para buscar al menos la ciberparidad en una eventual operación.

SCEPVA (Sovereing Cyber Effects Provided Voluntarily by Allies)

Como es bien sabido, salvo en casos muy particulares, la OTAN carece de fuerzas propias de combate, generándose las fuerzas para misiones y operaciones concretas por medio de la aportación voluntaria de las naciones (generación de fuerzas).

En el caso de las operaciones ofensivas en el ciberespacio, se ha considerado que el modelo vigente para la generación de fuerzas no resulta eficiente y se ha desarrollado uno específico que podríamos denominar de "generación de efectos", mediante el cual se crea una capacidad colectiva de ciberefectos para misiones y operaciones concretas a partir de la aportación voluntaria de las naciones (SCEPVA).

De una forma muy simplista, la OTAN planteará a los Estados participantes en esta iniciativa la posibilidad de llevar a cabo, en el marco de una operación, una acción ciberofensiva contra un determinado objetivo, quedando la responsabilidad del planeamiento y ejecución, con sus propios medios (soberanía), a cargo de la nación que recoja el guante. Es decir, la nación voluntaria no aportará una unidad ciberofensiva a la operación, sino los efectos sobre un objetivo.

En la actualidad, alrededor de una decena de naciones se han adherido a esta iniciativa, que se encuentra aún en fase de desarrollo.

Son varios los factores que han llevado a la OTAN a adoptar esta aproximación tan novedosa. Por una parte, las ciberoperaciones ofensivas continúan siendo en muchos de sus Estados Miembros un asunto muy controvertido, a pesar del reconocimiento general de que están sujetas a las mismas normas y principios del derecho internacional que las operaciones militares convencionales. Por otra, las naciones son todavía muy reacias a compartir sus capacidades de ciberdefensa, sobre todo en lo referente a las de obtención de inteligencia y ofensivas, trasladando a este ámbito un clima de opacidad y desconfianza que no existe en el resto de los dominios de las operaciones.

A priori, la idea puede no parecer mala. Las peculiaridades del ciberespacio llevan a que en la mayoría de las situaciones no sea ne-

cesario el despliegue en zona de unidades de la fuerza ciberespacial para generar los efectos deseados por el comandante de la misión. Así mismo, permite conseguir cierta capacidad disuasoria sin que los Estados tengan que revelar el contenido y naturaleza de sus arsenales de ciberarmas, ni sus técnicas y procedimientos.

Sin embargo, abandonando el plano teórico y enfrentándose a un caso concreto, resulta evidente que son muchas las cuestiones que quedan por resolver. La primera, lo farragoso y dilatado en el tiempo que puede resultar un proceso que involucrará a numerosos niveles y estamentos tanto del poder político como militar, tanto en cada Estado como en la propia estructura de la Alianza.

A pesar de que las películas y series nos animen a creer que un ciberataque se resuelve en cuestión de segundos, la realidad es muy otra. Una acción ofensiva en el ciberespacio requiere un análisis muy concienzudo del objetivo, que permita identificar vulnerabilidades explotables y posibles vectores de entrada, y que habrá de ser seguido por la preparación de las ciberarmas a emplear a medida del objetivo, ensayos, análisis de los posibles efectos colaterales,… Por lo general, una unidad ciberofensiva no podrá pronunciarse sobre si es capaz o no de combatir eficazmente un objetivo antes de un período de varias semanas o, incluso, meses. Y difícilmente podrá dar a la cadena de mando unas garantías razonables de que sus efectos no se extenderán más allá del objetivo.

Otras dudas que se plantean es cómo estos efectos, siendo soberanos, se integrarán en el mando y control aliado de las operaciones y cuál será la responsabilidad de la Alianza en su consecución, en especial si dan lugar a efectos no deseados o desproporcionados sobre infraestructuras críticas o servicios esenciales del adversario. Tampoco parece sencillo que se logre la aprobación política de los ciberefectos sin conocer previamente cómo se va a llevar a cabo el ataque.

Por lo tanto, no es descartable que esta singular y novedosa iniciativa acabe por no tener demasiados efectos prácticos y sea necesario volver al modelo tradicional u optar por nuevos planteamientos.

La idea: Standing NATO Cyber Force

Durante muchos años, la OTAN ha mantenido unas fuerzas navales de reacción inmediata, como parte de la NATO Response Force (NRF). *Los Standing NATO Maritime Groups 1 y 2*, herederos de las *Standing Naval Forces* del Atlántico y Mediterráneo (STANAVFORLANT y STANAVFORMED) se constituyen como grupos operativos navales con

el más alto grado de alistamiento y preparación, mediante las rotaciones de sus unidades componentes por períodos de varios meses.

Estos grupos navales están constituidos por un número variable de buques militares de diferentes países y, durante muchos años, han servido para incrementar el nivel de adiestramiento, depurar procedimientos, mejorar la interoperabilidad y fomentar la confianza y entendimiento entre las fuerzas navales de los Estados aliados. Los que hemos participado en estos grupos, hemos podido ver cómo la capacidad militar de nuestros buques alcanzaba su máximo nivel a medida que transcurrían los meses de despliegue. Al mismo tiempo, el contacto continuado tanto en puerto como en la mar promueve la aparición de lazos de amistad y confianza entre las dotaciones, creando un potente sentimiento de pertenencia al grupo.

La OTAN cuenta de esta forma con dos grupos navales permanentes, altamente cohesionados y operativamente muy potentes, en tanto las naciones se benefician del incremento de la capacidad operativa de sus unidades que lleva implícito su integración.

¿Por qué no tratar de aplicar este modelo de éxito al ciberespacio?

Analicemos qué haría falta.

En primer lugar, habría que aclarar de qué estamos hablando. ¿Qué es lo que habrían de aportar las naciones?

De forma muy resumida, una unidad ofensiva de ciberdefensa ha de contar con personal altamente especializado, un arsenal de ciberarmas (y cierta capacidad para producir otras nuevas o modificar las existentes), así como plataformas para su lanzamiento. Y, por supuesto, medios para su adiestramiento, tanto individual como colectivo, y entornos adecuados y convenientemente aislados para las necesarias pruebas y ensayos.

A mi entender, lo más valioso de las capacidades de ciberdefensa se encuentra en las personas. Es algo que puede resultar paradójico, pero mi experiencia acumulada no me deja duda alguna. A pesar de encontrarnos ante el dominio de las operaciones más altamente tecnificado y tecnológicamente más demandante, volátil y cambiante, las personas (especialistas) son el elemento más crítico y valioso. Por lo tanto, lo que habrán de aportar las naciones es, en primer lugar, personal experto y cualificado (talento). Se tiende a pensar que existen especialistas en ciberdefensa, sin más, que dominan toda la extensión de la disciplina. Nada más lejos de la realidad. Al igual que no hay especialistas navales sin más, y se requieren especialistas artilleros, electrónicos o maniobra y navegación a bordo de una fraga-

ta, la ciberdefensa requiere de personal de muy diferentes perfiles, lo cual es extensible a su vertiente ofensiva. Ello obligaría, como primer paso, a definir unos perfiles estándar, lo cual no resultaría demasiado complicado, pudiéndose utilizar como primera aproximación los habitualmente asociados a un *Red Team*[8].

La *Standing NATO Cyber Force* se constituiría, por lo tanto, a partir de una plantilla establecida según esos perfiles antes mencionados. Debería contar con un pequeño núcleo permanente, en tanto el resto debería ser cubierto por las naciones mediante aportaciones de personal que rotarían cada cierto número de meses (que no debería ser inferior a cuatro). En términos cuantitativos, esta unidad debería contar con una plantilla de unas 100-200 personas, teniendo en cuenta que en ocasiones podría tener que trabajar en régimen 24/7.

En lo referente a armamento e infraestructuras, la OTAN habría de poner a disposición de esta fuerza lo que podríamos denominar un "ciberarsenal estándar", contando con que el propio grupo, mediante el personal cualificado que lo integra, tenga capacidad para hacer las modificaciones pertinentes para adecuar las ciberarmas disponibles a un objetivo concreto. Así mismo, la organización deberá proveer a la fuerza de infraestructuras (muchas de ellas anonimizadas) para el "lanzamiento" de las armas, así como un campo de maniobras virtual (*cyberrange*) en el que puedan llevarse a cabo desde prácticas de adiestramiento individual y colectivo y ciberejercicios hasta los pertinentes ensayos de un ciberataque, reproduciendo el sistema objetivo con el máximo realismo posible.

Un elemento fundamental serán los procedimientos operativos, que habrá que desarrollar e ir depurando con el tiempo y la experiencia acumulada. Tampoco ha de ser un grave obstáculo, dado que muchas naciones tienen desarrollados los suyos y, seguramente, de forma muy similar.

El ciberespacio podría permitir que el personal constituyente de este equipo trabajara en red, y desde sus ubicaciones habituales. Sin embargo, estimo que sería muy beneficioso para la coordinación, cohesión y fomento de la confianza que trabajaran codo con codo en

---

(8) Equipo especializado en la ejecución de pruebas de penetración a sistemas TIC. Un Red Team imita las tácticas y técnicas que emplearía un atacante real contra las redes y sistemas de una organización, permitiendo detectar vulnerabilidades y fallos de seguridad que pueden ser explotados. En los ciberejercicios, se denomina así al equipo atacante, en tanto al defensor se le denomina Blue Team.

la misma ubicación. De hecho, considero este aspecto uno de los de mayor calado.

En cuanto a su encuadramiento orgánico, a mi entender lo ideal y más eficiente sería que tuvieran la condición de *NATO Response Forces*, dependiendo operativamente del recién constituido NATO CyOC *(Cyber Operations Center)*[9], ubicado en SHAPE[10] (Mons, Bélgica). No obstante, habrá que analizar cuidadosamente la relación de esta unidad con los comandantes de las operaciones a las que apoyen, a fin de lograr la mayor eficacia y eficiencia. Así mismo, deberá estar adecuadamente integrada en el complejo proceso de *targeting* de la OTAN.

Obviamente, la puesta en marcha de esta idea requiere un profundo cambio de mentalidad. Pero ya hay antecedentes. El *Locked Shields*, formidable ciberejercicio que cada año organiza el Centro Cooperativo de Excelencia en Ciberdefensa (CCD CoE), ubicado en Tallin (Estonia), constituye un potentísimo *Red Team* a partir de expertos locales y los que cada nación aporta, atendiendo a los perfiles que la organización solicita a fin de conformar adecuadamente los equipos. Muchos de los integrantes de estos Red Teams habrían de ser los mismos que constituyeran esa Standing NATO Cyber Force. Incluso, a pesar de la corta duración del ejercicio (que es compensada por su intensidad), los efectos de *Locked Shields* sobre los integrantes de estos equipos son muy parecidos a los que produce un despliegue SNMG en las dotaciones de los barcos en cuanto a camaradería y sentimiento de pertenencia al grupo.

A mi juicio, todo esto redundaría tanto en beneficio de la Alianza como de las propias naciones. Por un lado, la OTAN contaría permanentemente con una fuerza ofensiva en el ciberespacio alistada y preparada y reduciría los tiempos requeridos por los procesos derivados del modelo SCEPVA de generación de efectos; además, preservaría a las naciones de tener que asumir de forma aislada las responsabilidades que trae consigo su aplicación. Es indudable que tendría un efecto muy positivo sobre la preparación técnica y formación de sus

(9) En la Cumbre de Bruselas de 2018, se acordó la creación de un nuevo Centro de Operaciones en el Ciberespacio como parte de la Estructura de Mando de la OTAN. El objetivo de este Centro será proporcionar conocimiento de la situación *(cyber situational awareness, CySA)* y coordinación de la actividad operativa de la OTAN en el ciberespacio. Se prevé que alcance su capacidad operativa total (FOC) a lo largo del año 2023.

(10) *Supreme Headquarters Allied Powers Europe.*

componentes; y un atractivo especial para estos, en cuanto a lo que la pertenencia a este grupo de élite significaría en términos de prestigio profesional. Favorecería, así mismo, la adopción de procedimientos estándar y la interoperabilidad en las operaciones ciberofensivas. Y, por último, su propia existencia permitiría ir generando un clima de compañerismo entre sus integrantes que podría contribuir a eliminar progresivamente esa desconfianza y ocultación que concurren actualmente alrededor de la ciberdefensa ofensiva y que no existe en los ámbitos terrestre, naval o aéreo.

Reflexión final

Las operaciones ciberofensivas son una herramienta más a disposición de los comandantes para el cumplimiento de su misión, pero con unas características muy singulares. Por lo general, las acciones ciberofensivas no requieren de los enormes presupuestos, ni los despliegues de fuerzas característicos de las acciones convencionales. Además, es poco probable que un ciberataque provoque bajas en el adversario; y, casi imposible, en el bando propio. Por todo ello es presumible que una ofensiva en el ciberespacio sea contemplada de forma menos reticente que una acción militar convencional, tanto por el poder político como por la opinión pública.

Por otra parte, ya hemos visto lo complicado que resulta ejercer la disuasión en el ciberespacio. No hay ningún motivo para pensar que esa disuasión sea alcanzable por medios convencionales. En cuanto a la inversa, a mi juicio, el hecho de que un adversario cuente con unas sólidas y contrastadas capacidades ciberofensivas sí que puede influir sustancialmente en la decisión de llevar a cabo contra él acciones militares con medios convencionales.

Y si una marina de guerra o un ejército del aire de 25.000 hombres son los que corresponden a una potencia media en el concierto mundial, un ciberejército con unos pocos cientos de expertos en acciones ofensivas convierte a un Estado en una potencia considerable en el ciberespacio.

No cabe duda de que el ciberespacio va a tener cada vez más protagonismo en el devenir de los conflictos. Y el contar con unas potentes capacidades ciberofensivas (cuantitativa y cualitativamente) será tanto elemento esencial para disuadir al adversario como condición necesaria para el éxito en cualquier operación militar.

Bibliografía

AJP 3.20 Allied Joint Doctrine for Cyberspace Operations. (2020).

BENDIEK, Annegret & METZGER, Tobias. Deterrence theory in the cyber-century. (2015).

CHERTOFF, Michael & CILLUFFO, Frank J. Choosing to lead. American Foreign Policy for a Disordered World. Chapter 20: A strategy of cyber deterrence. (2015).

CIRENZA, Patrick. The flawed analogy between nuclear and cyber deterrence. (2016).

COLOM, Guillem. La OTAN despliega en el Ciberespacio. Revista Ejército. Octubre 2019.LIBICKI, Martin C. Cyberdeterrence and cyberwar. (2009).

GAITÁN RODRÍGUEZ, Andrés. El Ciberespacio: un nuevo escenario de batalla para los conflictos armados del siglo XXI. Escuela Superior de Guerra de Colombia. (2012).

GANUZA, Néstor. Guía de Ciberdefensa. Orientaciones para el diseño, planeamiento, implantación y desarrollo de una ciberdefensa militar. Junta Interamericana de Defensa. (2020).

GEERS, Keneth. The Challenge of Cyber Attack Deterrence. Computer Law & Security Review, 26(3), pp. 298-303. (2010).

LAN, Tang (y otros). Global Cyber Deterrence. Views from China, the U.S., Russia, India, and Norway. (2016).

LEWIS, James A. Cross-Domain Deterrence and Credible Threats. (2010).

NATO website: https://nato.int/ (última consulta: 16 de septiembre de 2020).

SCHMITT, Michael N. Grey Zones in the International Law of Cyberspace. (2017).

SCHMITT, Michael N. Tallinn Manual on the International Law Applicable to Cyber Operations. (2013).

SCHMITT, Michael N. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. (2017).

SIERS, Rhea. The Myth of Cyber Deterrence. (2016).

TORRES SORIANO, Manuel Ricardo. Los dilemas estratégicos de la ciberguerra. (2014).

TROMP, Joshua. Law of Armed Conflict, Attribution, and the Challenges of Deterring Cyber-attacks. (2010).

WEI, MAJ Lee Hsiang. The Challenges of Cyber Deterrence. (2015).