ieee.es
Instituto Español de Estudios Estratégicos
1970 — 2020

Documento
Opinión

51/2020 7 de mayo de 2020

Margarita Robles Carrillo *

La posición de Francia sobre el régimen jurídico de las operaciones en el ciberespacio

La posición de Francia sobre el régimen jurídico de las operaciones en el ciberespacio

Resumen

Francia ha definido su posición sobre el régimen jurídico de las operaciones en el ciberespacio en un documento, publicado en septiembre de 2019, bajo el título *Droit international appliqué aux operations dans le cyberspace* (DIAOC). El DIAOC establece el marco conceptual, el régimen aplicable a las operaciones cibernéticas en tiempos de paz y el derecho aplicable a las ciberoperaciones en situación de conflicto armado. Los principios básicos de la política francesa son dos: el cumplimiento del derecho internacional y la autoridad de Francia, en su condición de entidad soberana, para adoptar decisiones políticas sobre operaciones en el ciberespacio. El DIAOC constituye una aportación extraordinariamente relevante en un contexto marcado por los trabajos desarrollados en el marco de Naciones Unidas a través del nuevo Grupo de Expertos Gubernamentales (GEG) y del Grupo de Trabajo de Composición Abierta (OEWG).

Palabras clave

Francia, normativa, operaciones, ciberespacio.

France's position on the legal regime for transactions in cyberspace

Abstract

In September 2019, France has defined its position on the legal regime for operations in cyberspace in the document entitled Droit international appliqué aux operations dans le cyberspace (DIAOC). The DIAOC establishes the conceptual framework, the regime applicable to cyberoperations in times of peace and the law applicable to cyberoperations in situations of armed conflict. The basic principles of French policy are twofold: implementation of International Law and the authority of France, as a sovereign entity, to take political decisions on operations in cyberspace. It constitutes an extraordinarily relevant contribution in a context shaped by the work carried out within the framework of the United Nations through the new Group of Governmental Experts (GGE) and the Open-Ended Working Group (OEWG).

Keywords

France, regulation, operations, cyberspace.

Introducción

El régimen jurídico de las operaciones en el ciberespacio está siendo objeto de debate en el marco de Naciones Unidas, desde hace tiempo, a través de distintos órganos, sin que se haya alcanzado aún el necesario consenso entre los Estados. Antes, al contrario, hay un creciente desacuerdo que se manifiesta en el fracaso del Grupo de Expertos Gubernamentales (GEG) de 2017 y en la adopción en 2018 por la Asamblea General (AGNU) de dos resoluciones distintas en las que se establecen dos grupos de trabajo diferentes por su naturaleza, composición y funcionamiento: un nuevo GEG[1] y un Grupo de Trabajo de Composición Abierta (OEWG)[2]. El primero es intergubernamental y restringido, mientras que el segundo, también intergubernamental, es multilateral y cuenta con un componente *multistakeholder* del que carece el GEG.

El disenso entre los Estados se manifiesta principalmente en el hecho de que los que votaron a favor del primer grupo —encabezados por Estados Unidos y los miembros de la Unión Europea—, se pronunciaron en contra del segundo —defendido por la Federación Rusa y China— y a la inversa. Ello supone la ruptura del acuerdo básico primigenio que existía sobre el modelo y los procedimientos de trabajo y la apertura de una nueva etapa plagada de dudas e interrogantes, entre otros, sobre el alcance, el contenido y el valor de los informes que han de presentar a la AGNU. Mientras tanto, muchos Estados están adoptando políticas y medidas nacionales sobre la normativa aplicable a las operaciones en el ciberespacio. Si bien expresan su conformidad con el ordenamiento jurídico internacional, esas acciones estatales responden a la propia concepción nacional sobre la materia y suponen necesariamente una reinterpretación de aquel sistema normativo por el mero hecho de su traslación al ciberespacio.

En septiembre de 2019, en Francia, el Ministère des Armées ha hecho público el documento «Droit international appliqué aux operations dans le cyberspace» (en adelante, DIAOC) donde se explica la posición de este país sobre la materia[3]. Aunque otros Estados han adoptado normas y estrategias al respecto, el análisis del DIAOC es importante por varios motivos: 1) Francia es un sujeto internacional con un estatuto

[1] A/RES/73/266, de 22 de diciembre de 2018.
[2] A/RES/73/27, de 5 de diciembre de 2018.
[3] «Droit international appliqué aux operations dans le cyberspace». París: Ministère des Armées, 2019 (en adelante, DIAOC).

jurídico y un protagonismo contrastado en el desarrollo de esta normativa[4], que ha participado en todos los GEG y tiene representación en el nuevo GEG y en OEWG; 2) Francia, en su condición de miembro de la Unión Europea, constituye una referencia ineludible para el resto de los países en los temas de seguridad y defensa donde, históricamente, ha defendido la construcción de una política europea; 3) el objetivo del DIAOC es explicar la política nacional con el propósito declarado de contribuir al desarrollo de la cooperación internacional; 4) los principios rectores del DIAOC, presentes a lo largo de todo el texto, son el cumplimiento del derecho internacional y la autoridad de Francia, en su condición de entidad soberana, para adoptar decisiones políticas sobre operaciones en el ciberespacio, de manera que constituye una aportación relevante sobre la combinación de ambos elementos; y 5) el DIAOC rechaza implícita y expresamente, en varios y significativos aspectos, la interpretación realizada en el marco doctrinal a través del manual de Tallin que, para muchos, ha sido el marco principal de referencia en la materia[5]. La posición de Francia sobre régimen jurídico de las operaciones en el ciberespacio merece, por las razones indicadas, ser objeto de análisis. Para empezar, hay que abordar el marco conceptual sobre el que se basa el DIAOC.

Marco conceptual

El DIAOC se apoya en un marco conceptual definido en su glosario que presenta algunos problemas y carencias, en particular, en la definición de los conceptos de ciberarma, ciberataque y ciberoperaciones.

[4] Francia es miembro permanente del Consejo de Seguridad de Naciones Unidas, ha participado en todos los grupos de expertos gubernamentales de Naciones Unidas (GEG) sobre el tema, es miembro asimismo de las principales organizaciones y foros con competencias en la materia y ha protagonizado algunas iniciativas relevantes como el *Appel de Paris pour la confiance et la sécurité dans le cyberespace*. Disponible en https://www.diplomatie.gouv.fr/IMG/pdf/texte_appel_de_paris_-_fr_cle0d3c69.pdf.
[5] SCHMITT, M. (dir.). *The Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press, 2013. SCHMITT, M. y VIHUL, L. (dir.). *The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press, 2017.

Ciberoperaciones

El concepto de ciberoperaciones y su uso a lo largo del DIAOC no están correctamente resueltos[6]. Las ciberoperaciones son definidas como «actions de lutte informatique défensive (LID), de lutte informatique offensive (LIO), ou de cyber renseignement». La LID se concibe como «ensemble coordonné d'actions menées par un État qui consiste à détecter, à analyser et à prévenir des cyberattaques, et à y réagir le cas échéant». La LIO se define como «ensemble des actions entreprises dans le cyberespace produisant des effets à l'encontre d'un système adverse, pour en altérer la disponibilité ou la confidentialité des données».

Estas definiciones plantean, principalmente, dos problemas. El primero es que la LID se circunscribe a acciones realizadas por un Estado, mientras que no hay referencia a la autoría en el caso de la LIO, lo que permitiría incluir dentro de la misma acciones realizadas por agentes no estatales. Probablemente tendría más sentido permitir ese tipo de intervención en actividades defensivas en lugar de en las ofensivas. El segundo problema es que la LIO se limita a acciones destinadas a alterar la disponibilidad o confidencialidad de los datos excluyendo, inexplicablemente, en su propia definición la posibilidad de acciones ofensivas con una finalidad o funcionalidad distintas. Mientras, la LID tiene un ámbito de acción más amplio, incluida la capacidad de reaccionar sin esa limitación que se establece en la LIO, ni ninguna otra específica. Esas diferencias conceptuales sobre la autoría y el ámbito de actuación no se justifican, ni tampoco son suficientes para apreciar la verdadera diferencia entre ambas categorías.

Ciberarma

La ciberarma se define como «moyen(s) numérique(s), à l'inclusion des armes, des moyens et des méthodes de guerre numériques, mis en œuvre dans une cyberopération menée à l'encontre de la partie adverse en contexte de conflit armé et en lien avec celui-ci». El problema principal de esta definición es que no se trata de un concepto autónomo, sino que está vinculado a la realización de una ciberoperación, contra un adversario, en

[6] En la nota 1 se advierte que «les expressions «opérations dans le domaine cyber», «cyberopérations» et «opérations cyber» sont considérées comme des synonymes. Pour les définitions associées, voir le glossaire en annexe» (DIAOC, p. 4).

el contexto de un conflicto armado y en conexión con el mismo. Ello plantea algunos problemas.

En primer lugar, el concepto de ciberarma está limitado objetiva y contextualmente a la existencia de una situación de conflicto armado. Ello excluye la posibilidad de calificar como ciberarmas el uso de medios cibernéticos en el marco de una ciberoperación contra un tercero si no se realiza dentro de un conflicto armado y vinculado al mismo. Es un concepto solo operativo dentro del *Ius in bello*, pero no respecto del *Ius ad Bellum*. No sirve, en consecuencia, para determinar la existencia de una amenaza o un uso de la fuerza armada, un ataque armado o una agresión previos a la existencia del conflicto bélico. Al no ser válido a esos efectos, se plantean dos problemas: por una parte, se requeriría la formulación de un concepto de ciberarma al margen o fuera de la situación de conflicto armado; y, por otra parte, supondría tener que operar con dos conceptos diferentes, según existiese o no esa situación de conflicto, incluso cuando el usuario, el adversario, el medio y los efectos fuesen idénticos, solo por el hecho de que esta definición se ha circunscrito a ese contexto. Para evitar estos problemas, el concepto de ciberarma debería ser un concepto autónomo, independiente de su utilización en una situación concreta, en tiempos de paz o de conflicto.

En segundo lugar, el concepto de ciberarma está limitado funcionalmente a su uso dentro de una ciberoperación. Esta, aparentemente inocua, vinculación también resulta problemática si se atiende a la definición de ciberoperación realizada en el DIAOC. Como se ha visto en el punto anterior, las ciberoperaciones son acciones de lucha informática defensiva (LID), ofensiva (LIO) o de ciberinformación/ciberinteligencia. En principio, esta tercera modalidad no necesariamente debería implicar el uso de ciberarmas. En la LID, solo incluiría aquellas usadas por un Estado. En la LIO solo abarcaría aquellas destinadas a alterar la disponibilidad o confidencialidad de los datos. La cuestión estriba en que, para ser una ciberarma, ha de ser usada en una ciberoperación pero, atendiendo a las tres modalidades previstas, en el caso de la LID, obligaría a que el usuario fuese un Estado, en el caso de la LIO, exigiría que su finalidad fuese alterar la disponibilidad o confidencialidad de los datos y, en el último supuesto, podría conducir a calificar como ciberarma cualquier acción cibernética destinada a operaciones de información o inteligencia. Combinar las definiciones de ciberarma, ciberoperación, LID y LIO es un ejercicio imposible de interpretación jurídica e, incluso, inmanejable en términos políticos, militares u operativos.

En definitiva, la definición de ciberarma del DIAOC no ofrece un concepto general en cuanto a su contenido, ni en cuanto a su aplicación porque está limitado a la situación de conflicto armado. Las condiciones en las que se establece en el marco de una ciberoperación complican, adicionalmente, su operatividad práctica incluso en ese contexto. A ello se le suma el hecho de que esa definición parece ajustarse en mayor medida a la idea de ciberataque armado, pero en el DIAOC no se vincula al mismo. El concepto de ciberataque tampoco es un ejemplo de precisión conceptual.

Ciberataque

El ciberataque es definido en el DIAOC como la «action volontaire, offensive ou malveillante, menée au travers du cyberespace et destinée à provoquer un dommage (en disponibilité, intégrité ou confidentialité) aux données ou aux systèmes qui les traitent, pouvant ainsi nuire aux activités dont ils sont le support. Une cyberattaque peut être une cyberopération conduite par un Etat contre les intérêts de l'Etat français». Esta definición no encaja fácilmente con los demás conceptos, ni con la materia misma objeto de DIAOC. El DIAOC opera con un concepto de ciberataque excesiva e injustificadamente genérico, amplio en un sentido (A) y restrictivo en otro (B), que no resulta coherente con el resto de las categorías definidas en el mismo (C).

A) El concepto de ciberataque es genérico porque permite englobar dentro del mismo cualquier acción cibernética que reúna las características indicadas, desde el mero activismo hasta cualquier hecho ilícito de carácter delictivo, excepto precisamente una acción contraria a la prohibición del uso y de la amenaza de la fuerza o constitutiva de un acto de ciberguerra porque prescinde de dos componentes básicos a esos efectos: la naturaleza «armada» del ciberataque y el carácter «internacional» del mismo. Por una parte, el ejemplo de una operación de un Estado contra Francia no es, en sentido preciso, parte de la definición, ni parece suficiente para situar ese concepto de ciberataque en el marco de una relación internacional, que es una condición básica para aplicar el *Ius ad bellum* y el *Ius in bello* en el marco de una operación en el ciberespacio. Por otra parte, mientras el concepto de ciberarma está claramente vinculado a una actividad de naturaleza bélica y a una ciberoperación «menée à l'encontre de la partie adverse en contexte de conflit armé et en lien avec celui-ci», el ciberataque se sitúa «au travers du cyberespace». No es, en consecuencia, un concepto preciso para definir un ciberataque

en el sentido del modelo de seguridad colectiva de Naciones Unidas o dentro del DICA, ni siquiera resulta fácil combinarlo con el concepto de ciberarma para determinar la existencia de un ciberataque armado.

B) La definición de ciberataque se limita a acciones ofensivas, lo que excluye la posibilidad de incluir dentro de esa categoría operaciones de naturaleza defensiva. Es una limitación del alcance de ese concepto difícilmente explicable por sí misma y en el contexto general del DIAOC porque, cuando define la ciberdefensa militar, contempla tanto acciones ofensivas como defensivas y, cuando conceptúa las ciberoperaciones, distingue entre acciones defensivas (LID) y ofensivas (LIO). El Protocolo Adicional I a los Convenios de Ginebra (en adelante, PAI), en su art. 49, incluye expresamente en el concepto de «ataques» los actos de violencia contra el adversario tanto ofensivos como defensivos.

C) El concepto de ciberataque no resulta coherente con el resto de las definiciones realizadas en el DIAOC como las de ciberarma, ciberdefensa, ciberdefensa militar o ciberoperaciones desde el punto de vista de los contenidos o de los sujetos implicados en la operación. En todas ellas, hay un componente defensivo que está ausente en el concepto de ciberataque. En todas ellas, desde el punto de vista subjetivo, se trata de partes adversarias o de Estados, mientras que se prescinde del elemento de autoría en la noción de ciberataque.

En términos jurídicos, el problema principal estriba en que, desde la perspectiva de las operaciones en el ciberespacio en el contexto del *Ius ad bellum* y el *Ius in bello*, el concepto de «ciberataque armado» es esencial porque es el presupuesto para activar esa normativa internacional que es objeto de análisis en el DIAOC, pero resulta extraordinariamente difícil articularlo a partir de las definiciones de ciberarma y de ciberataque adoptadas en el mismo y tampoco ayudan el resto de las definiciones incluidas en el DIAOC.

En definitiva, atendiendo a estas nociones básicas, la conclusión es que el marco conceptual del DIAOC presenta serias carencias que van a afectar necesariamente a la comprensión de régimen normativo previsto en el que se diferencia entre operaciones en tiempos de paz y en situación de guerra.

Ciberoperaciones en tiempos de paz

La sección del DIAOC relativa a las ciberoperaciones contra Francia en tiempos de paz consta de tres secciones[7]. No obstante, se comprende mejor si, prescindiendo de esa estructura, se identifican las tres posibles situaciones con las que opera en función de que se produzca un ciberataque constitutivo de una violación de soberanía, una violación de la prohibición de recurrir al uso o a la amenaza de la fuerza o un ataque armado. La obligación de diligencia debida y el régimen de atribución completan esta parte.

Violación de la soberanía

El DIAOC dispone que un ciberataque puede constituir una violación de la soberanía del Estado, pero es preciso determinar el alcance del principio de soberanía en el ciberespacio porque se trata de un concepto vinculado al ejercicio de una competencia territorial sobre un espacio físico por parte del Estado.

El DIAOC establece que el principio de soberanía implica la competencia territorial tradicional y una competencia territorial en materia de infraestructuras informáticas. Aunque en el texto se refiere expresamente a los «sistemas de información situados sobre su territorio», en una nota a pie de página incluye dentro de esta expresión «los equipamientos e infraestructuras franceses o de interés francés». Esta puntualización supone una extensión tan considerable como cuestionable del ámbito de actuación posible de Francia bajo la cobertura del principio de soberanía[8].

Sobre esa discutible base, el DIAOC identifica dos supuestos: un ataque contra los sistemas digitales franceses o un ataque que produzca sus efectos sobre el territorio francés. En ambos casos, la autoría es fundamental porque ha de ser realizado por una persona o una entidad en el ejercicio de prerrogativas de poder público o por una persona o personas actuando bajo las directrices, las instrucciones o el control de un Estado. El DIAOC dedica una atención específica a la injerencia mediante una operación digital en los asuntos internos o externos o en los sistemas digitales estatales, que califica como una violación del principio de no intervención en los asuntos internos derivado de la

[7] En la primera sección se declara que Francia se reserva el derecho a responder a todo ciberataque constitutivo de una violación de derecho internacional de la que sea víctima. En la segunda se establece que un ciberataque que provoque daños de una amplitud y gravedad significativa puede constituir una agresión armada que autorice el uso de la legítima defensa. En la tercera se dispone que la atribución de un ciberataque de origen estatal constituye una decisión política nacional (DIAOC, pp. 6-11).
[8] El Informe del GEG de 2015 afirma el principio de soberanía y la jurisdicción «sobre las infraestructuras de TIC ubicadas en su territorio» (A/70/174, de 22 de julio de 2015, p. 15). La inclusión de la categoría «interés» no forma parte del consenso alcanzado en el marco de Naciones Unidas.

soberanía. Como reacción, se contempla la posibilidad de operaciones de lucha informática defensiva incluida la neutralización de los efectos del ciberataque.

Siguiendo el DIAOC, la respuesta frente a un ciberataque constitutivo de una violación de la soberanía se realizará considerando la naturaleza, las características y la gravedad de la intrusión y teniendo en cuenta las diversas opciones que permite el derecho internacional, junto con criterios de oportunidad decididos por las autoridades políticas.

Vulneración de la prohibición del uso o de la amenaza de la fuerza

Una acción cibernética puede constituir una violación de la prohibición de uso o de amenaza de la fuerza armada contra la integridad territorial o la independencia política de Francia.

El principio establecido en el DIAOC es que un ciberataque realizado por un Estado contra otro Estado constituye una violación de dicho principio si los efectos son similares a los resultantes del uso de un arma clásica. Ello no implica excluir aquellos supuestos en los que no se produzcan efectos físicos porque existen otros criterios evaluables para la determinación de la existencia de un uso o amenaza de la fuerza. Reconociendo que no se trata de una lista exhaustiva, el DIAOC incluye entre esos criterios: las circunstancias de la operación —el origen o la naturaleza del instigador—, el grado de intrusión, los efectos provocados o pretendidos o la naturaleza del objetivo.

Las respuestas posibles en caso de un ciberataque de esta naturaleza serían: 1) la adopción de contramedidas individuales, en su condición de víctima, conforme al derecho internacional, de naturaleza pacífica y dirigidas al cese de la violación, pero incluyendo una posible derogación del requisito de notificación previa en caso de urgencia o por la necesidad de proteger sus derechos; 2) el recurso al Consejo de Seguridad de Naciones Unidas en virtud de los capítulos VI y VII de la Carta; o 3) la invocación del estado de emergencia o de necesidad para proteger un interés esencial.

En ese marco jurídicamente legítimo, la decisión sobre la medida a adoptar es de naturaleza política. El problema estriba en que, en ese mismo punto, se advierte que Francia dispone de medios de prevención, anticipación, protección, detección y reacción frente a ciberataques constitutivos de una violación del derecho internacional de la que sea víctima. La capacidad de responder con ciberoperaciones sería legítima en algunas

de esas circunstancias, pero resulta difícilmente justificable en los supuestos de «prevención» y «anticipación».

Ataque armado

El DIAOC reconoce que una acción cibernética puede constituir un ataque armado en el sentido del artículo 51 de la Carta de Naciones Unidas. Con carácter general, se mantiene el mismo criterio que en el caso anterior porque se atiende al hecho de que los efectos de la operación sean similares a los de un ataque con armamento clásico. Pero, además, se enumeran algunos posibles supuestos: pérdidas humanas sustanciales, daños físicos o económicos considerables o afectación de infraestructuras críticas con consecuencias significativas o susceptibles de paralizar ámbitos de actividad o desencadenar catástrofes tecnológicas o ecológicas.

En este supuesto, cabría la posibilidad de ejercer la legítima defensa individual o colectiva por medios cibernéticos o clásicos siempre que se respeten los principios de necesidad y proporcionalidad. El DIAOC reconoce, en casos excepcionales, la posibilidad de recurrir a la legítima defensa *préemptive*, en los términos establecidos en derecho internacional, pero excluye la legalidad de la denominada preventiva.

La obligación de diligencia debida

El DIAOC se ocupa del problema específico que plantea el incumplimiento por parte de un Estado de la obligación de diligencia debida cuando se utiliza su territorio, en particular por agentes no estatales, para cometer hechos internacionalmente ilícitos a través de las TIC[9].

Los Estados deben velar por evitar ese tipo de situaciones y prácticas, pero el incumplimiento de esta obligación solo autoriza la activación de mecanismos diplomáticos y, de ser necesario, la adopción de contramedidas o el recurso al Consejo de Seguridad. No permite, en cambio, el ejercicio de la legítima defensa contra dicho

[9] El problema estriba en que la diligencia debida no es un concepto jurídico claramente definido en derecho internacional. Como explica McDonald, «The nature of the role of due diligence in international law depends on the context. Acting with due diligence can be explicitly required under a rule, be part of a rule, or be required by necessary implication to act in conformity with a rule. But there is no general rule or principle of due diligence in international law» (McDONALD, N. «The Role of Due Diligence in International Law». *International and Comparative Law Quarterly*, vol. 68. 2019, p. 1054).

Estado porque el incumplimiento de aquella obligación no constituye una excepción a la prohibición del uso o de la amenaza de la fuerza. En este punto, el DIAOC es contundente en su crítica a la mayoría de los expertos del manual de Tallin que defienden la legítima defensa contra el Estado que no ha cumplido ese deber de diligencia. Esta posibilidad está excluida, según los términos del DIAOC, incluso si la respuesta fuese respetuosa con el principio de necesidad, si fuese el único modo de hacer frente a la agresión y si el Estado territorial no quisiese o no estuviese en condiciones de impedir la realización de esas actividades.

Atribución del acto

Tras analizar los criterios y parámetros para la calificación y la respuesta en función de esas distintas posibilidades, el DIAOC establece que la atribución de la autoría del ciberataque es una decisión de política nacional[10].

En principio, conforme al derecho internacional, un ciberataque es considerado un hecho de un Estado si ha sido perpetrado por un órgano estatal, una persona o entidad en el ejercicio de prerrogativas de poder público o una persona o un grupo de personas actuando bajo las instrucciones, directivas o control del Estado al que se atribuirá el hecho en cuestión. La atribución se realizará teniendo en cuenta, en particular, la naturaleza y el origen de la operación, las circunstancias del caso o el contexto internacional. A esos efectos se consideran relevantes los elementos técnicos y operativos como la determinación de la infraestructura de ataque o de tránsito, la identificación del *modus operandi*, la cronología, la extensión, la amplitud, la gravedad, el perímetro comprometido o, incluso, los efectos queridos por el atacante. Al tratarse de una decisión soberana, Francia se reserva la posibilidad de hacerla o no pública a su población, a otros países o a la comunidad internacional. No se excluye la posibilidad de una atribución colectiva realizada en el marco de organizaciones como la UE o la OTAN, pero reivindica la competencia nacional.

Desde esa perspectiva, cabe destacar dos elementos: la definición de la atribución como una competencia exclusiva del Estado y la afirmación de que el derecho internacional no

[10] El informe del Senado sobre la soberanía digital afirma que «l'attribution publique est une décision politique qui relève de la souveraineté et ne peut être faite par une structure multinationale, qu'elle soit interalliée comme l'OTAN ou autre» (*Rapport sur la souveranité numérique*. Octubre 2019, p. 114).

obliga a comunicar los elementos de prueba sobre la base de los cuales se realiza la atribución, si bien esos elementos permiten legitimar dicha atribución. Ello lleva a la conclusión de que «le défaut d'attribution publique ne constitue pas un obstacle définitif à l'application du droit international, notamment à la mise en œuvre du droit de réponse offert aux États».

En realidad, esta declaración debe ser matizada porque, como se reconoce en el propio DIAOC, en función de la calificación del ciberataque, la respuesta es diferente y se encuentra regulada por el ordenamiento jurídico internacional. Si se trata de contramedidas, existe un procedimiento, unos requisitos y unos límites jurídicos a su aplicación. Si se trata de acudir a los capítulos VI o VII de la Carta de Naciones Unidas, hay unas reglas y un procedimiento establecidos normativamente de carácter obligatorio. Si se trata de ejercer la legítima defensa, el art. 51 de la Carta establece asimismo las condiciones y el procedimiento. En consecuencia, solo la respuesta diplomática —cuyo alcance y contenido es, por naturaleza limitado—, podría realizarse sin una atribución pública. En el resto de los casos, las propias condiciones que impone el derecho internacional para la respuesta implican *de facto* la conversión en pública de esa operación —la atribución del hecho ilícito—, con independencia de que se realice de modo expreso o se infiera implícitamente como consecuencia de la puesta en marcha de cualquiera de esos mecanismos de respuesta.

Ciberoperaciones en tiempos de conflicto

El ciberespacio es un espacio de confrontación en el que se aplican las normas del DICA. Con este planteamiento de principio, que encuentra luego algunas matizaciones, la segunda sección del DIAOC se estructura en tres apartados[11]. Como en el caso de la primera, para su mejor comprensión es conveniente explicarla atendiendo a los contenidos: la relación entre ataque y conflicto armado y la aplicación de los principios del DICA.

[11] La segunda sección se divide en tres apartados: las ciberoperaciones pueden caracterizar la existencia de un conflicto armado, el derecho internacional humanitario (DIH) se aplica a las ciberoperaciones en el contexto de un conflicto armado o vinculadas con el mismo y el derecho de la neutralidad tiene vocación de aplicarse en el ciberespacio (DIAOC, pp. 12-17).

Ataque y conflicto armado

Las reglas existentes en el mundo precibernético para calificar una acción cibernética como un ataque armado o para determinar la existencia de un conflicto armado no son fácilmente extrapolables al ciberespacio. El DIAOC analiza dos cuestiones: la calificación de una operación cibernética como un ataque armado (a) y la capacidad de esas operaciones para determinar la existencia de un conflicto armado (b).

a) La calificación de una operación como un ataque armado es un problema que ha sido objeto de muy diversas opiniones doctrinales. El DIAOC considera ataque, en el sentido del art. 49 del Protocolo Adicional I (PAI) a los Convenios de Ginebra, «toute cyber-opération menée en contexte de conflit armé, en lien avec celui-ci et constitutif d'un acte de violence, offensif ou défensif, contre une autre partie au conflit»[12]. En consecuencia, los parámetros para la determinación del ataque son tres: uno, contextual, que es la existencia de un conflicto armado; otro funcional, que viene dado por el vínculo de la operación en cuestión con ese conflicto; y un tercero, material, que es la definición de dicha operación como un acto de violencia. Todos y cada uno de ellos son susceptibles de interpretación.

El elemento determinante, sin embargo, viene dado a continuación cuando el DIAOC advierte que Francia no comparte la interpretación realizada en el manual de Tallin sobre el concepto de ataque sobre la base de criterios materiales y resultados definitivos o temporales, sino que adopta expresamente un criterio funcional. En dicho manual, el ciberataque se asocia a daño o muerte en las personas o daño o destrucción en las cosas. En cambio, el DIAOC adopta una definición de ataque que no se basa en esos resultados, ni tampoco en el carácter temporal o definitivo, reversible o no de los mismos. La posición de Francia consiste en considerar que una operación cibernética constituye un ataque en el sentido del art. 49 del PAI cuando los equipamientos o los sistemas objeto de esta dejan de prestar el servicio para el que fueron establecidos y se requiere una intervención para restablecer el funcionamiento de la infraestructura o el sistema. El criterio funcional desplaza al criterio material defendido en el manual de Tallin.

b) La cuestión de la capacidad de las operaciones cibernéticas para determinar la existencia de un conflicto armado no está claramente resuelta en el DIAOC. En un primer apartado se afirma que las ciberoperaciones constitutivas de hostilidades entre dos o

[12] DIAOC, p. 13.

más Estados podrían servir para caracterizar la existencia de un conflicto armado internacional (CAI) mientras que, en el resto de los casos, donde se opongan otras categorías de agentes, fuerzas o grupos armados, con un mínimo de organización y un determinado grado de violencia, se trataría de un conflicto armado no internacional (CANI). Esta distinción podría interpretarse como la aceptación de la capacidad de la acción cibernética por sí sola para determinar la existencia de un conflicto armado, esto es, reconocer la posibilidad de existencia de un conflicto cibernético como fenómeno autónomo. Pero, en realidad, no es tan sencillo por dos motivos principales.

El primero es que, a continuación, el DIAOC identifica dos posibles situaciones: por una parte, las operaciones cibernéticas concurrentes con operaciones militares convencionales que constituirían la regla general y menos problemática dado que la situación de conflicto ya vendría definida y caracterizada como tal por la presencia del componente físico convencional; y, por otra parte, las operaciones cibernéticas autónomas que, aunque no se excluyen, se consideran una hipótesis menos probable por cuanto habrían de alcanzar el nivel de violencia necesario para admitir tal calificación[13]. El segundo motivo es que se reconoce expresamente que los medios cibernéticos son «tout d'abord, des moyens de combinaison et de soutien des effects conventionnels»[14].

El problema estriba en que el DIAOC parte de la base de que las operaciones cibernéticas autónomas son la excepción cuando, si no lo son ya, están destinadas a convertirse en la regla. Es cierto que son numerosos los obstáculos que plantea su identificación, atribución y calificación como acción armada. Es cierto que no ha habido una declaración o un reconocimiento expreso de un acto de esa naturaleza. Pero si la conflictividad cibernética crece exponencialmente en todas sus modalidades y si, dentro de ella, se identifican acciones de las que son autores o víctimas los Estados, resulta difícil creer que las operaciones cibernéticas de naturaleza bélica vayan a limitarse a ser una excepción o un simple complemento respecto del conflicto convencional.

[13] Según el DIAOC, «L'état de la technologie semble exclure pour le moment que des cyber-opérations seules puissent atteindre le seuil de violence requis pour caractériser une situation de CANI» (DIAOC, p. 13).
[14] DIAOC, p. 13.

La aplicación de los principios del DICA

La aplicación de los principios del DICA en el ciberespacio ha sido generalmente reconocida en el marco internacional. El informe del GEG de 2015 confirma expresamente los principios de humanidad, necesidad, proporcionalidad y distinción[15]. Distinción, proporcionalidad y precaución son los principios que, según el Comité Internacional de la Cruz Roja, pueden y deben ser respetados[16]. El DIAOC incluye los principios de distinción, proporcionalidad, precaución y neutralidad.

El art. 48 del PAI establece la obligación de las partes en conflicto de distinguir entre población civil y combatientes y entre bienes civiles y objetivos militares. Por ello, de acuerdo con el DIAOC, están prohibidos los ciberataques que no estén dirigidos contra un objetivo militar o cuyos efectos no puedan ser limitados. En caso de duda sobre la condición civil o militar, las reglas son las siguientes: la persona ha de ser considerada civil y hay una presunción de que el bien normalmente destinado a un uso civil no va a ser utilizado para aportar una contribución efectiva a la acción militar. En este punto, hay una diferencia significativa respecto del manual de Tallin que, en caso de duda sobre la finalidad del uso del bien civil, habilita la opción de atribuirle una finalidad militar sobre la base de un examen minucioso del mismo. Esa posibilidad está excluida expresamente y en términos operativos en el DIAOC.

La distinción entre objetivos militares y bienes civiles se realiza por exclusión. Son considerados civiles todos los bienes que no constituyen objetivos militares. Pueden ser objetivos militares los datos, los procesos, el tráfico, los servicios, los sistemas o los equipamientos informáticos en dos supuestos concretos: si contribuyen a la acción militar por su naturaleza, localización, destino o utilización o si su destrucción, captura o neutralización otorgan una ventaja militar precisa. A pesar de la contundencia en su formulación, no resultan ser criterios fácil y objetivamente aplicables. Existe, no obstante, la garantía que ofrecen los procedimientos establecidos para identificar la naturaleza del objetivo y se ofrecen algunos ejemplos que pueden ayudar a clarificar la situación. Entre ellos, se identifican bienes especialmente protegidos por razones médico-sanitarias, culturales, medioambientales, por razones de subsistencia o por el peligro que encierran, así como a los datos, procesos y servicios necesarios para su mantenimiento. Esta

[15] A/70/174, de 22 de julio de 2015, p. 16.
[16] CICR. *International humanitarian law and the challenges of contemporary armed conflicts*. Ginebra: 2019, p. 20.

precisión es importante porque, nuevamente, Francia se aparta expresamente de la opinión manifestada por los expertos del manual de Tallin porque entiende que la protección dispensada a esos bienes especiales se extiende a los sistemas y datos que garantizan su funcionamiento[17].

La distinción entre civiles y combatientes se realiza, asimismo, por exclusión. El concepto de cibercombatientes comprende el personal militar, los grupos de *hackers* bajo control estatal y los miembros de grupos armados organizados salvo si están fuera de combate. El resto es considerado y protegido frente a las operaciones militares, salvo si participa directamente en las hostilidades y durante el tiempo de esa participación.

La aplicación de los restantes principios del DICA no es objeto de un desarrollo tan detallado. En el caso del principio de proporcionalidad, más allá de su caracterización genérica, hay un reconocimiento de las condiciones singulares que plantea a esos efectos el ciberespacio y de la necesidad de atender al conjunto de daños previsibles por el uso de la operación en cuestión, tanto directos como indirectos. Entre los aspectos destacables se encuentra la propuesta de desarrollo de ciberarmas específicas cuya utilización pueda decidirse en función de los efectos pretendidos en cada situación. La ausencia de control, la irreversibilidad o la interrupción temporal sin ventajas militares serían contrarios a este principio. El principio de precaución se limita al desarrollo de operaciones LIO y a una sucinta descripción del procedimiento a seguir en ese contexto.

Por su parte, sobre el principio de neutralidad, el DIAOC reconoce que implica obligaciones para las partes en conflicto y para el Estado neutral, que debe impedir el uso de las infraestructuras situadas en su territorio o bajo su control por los beligerantes, salvo si se trata de mera comunicación. Pero un ciberataque a través de los sistemas del Estado neutral sin efectos sobre el mismo no sería contrario a la neutralidad que solo prohíbe el tránsito físico. Esta interpretación, excesivamente apegada al concepto de conflicto físico, no parece reconocer las consecuencias que puede tener el tránsito virtual a través de un espacio neutral en el desarrollo del conflicto.

[17] DIAOC, p. 16.

Conclusiones

El DIAOC establece la posición de Francia sobre el régimen jurídico de las operaciones en el ciberespacio. El análisis de este permite identificar algunos aspectos negativos, en particular, los tres siguientes: 1) los problemas conceptuales dificultan tanto la comprensión como la aplicación de esa normativa. No solo es cuestionable la definición de los conceptos de ciberarma, ciberataque, ciberoperaciones, LID o LIO, incluso ciberdefensa o ciberdefensa militar, sino que no existe la cohesión mínima necesaria entre esas nociones; 2) hay una apreciable falta de coherencia entre la parte conceptual y la parte dispositiva del DIAOC como demuestra, particularmente, el uso de los conceptos de ciberataque o ciberoperación; y 3) hay un recurso excesivo a la ejemplificación en determinados aspectos, como en el principio de distinción, que aminora el potencial del DIAOC como instrumento de referencia en la materia. Entre las carencias destaca, particularmente, la definición de ciberarma.

El concepto de ciberarma es una categoría jurídica esencial para el derecho internacional desde una triple perspectiva. Primero, dentro del sistema de seguridad colectiva diseñado en la Carta de Naciones Unidas, ese concepto es clave para calificar una acción o una operación cibernética como una violación de la prohibición del uso o de la amenaza de la fuerza armada, un ataque armado o una agresión, con las consecuencias jurídicas que de ello se derivan. Segundo, en el marco de una situación de conflicto armado, el diseño y el uso de una ciberarma está sometido al régimen jurídico del DICA. Tercero, la definición de ciberarma es básica para la articulación de una política de control armamentístico en el ciberespacio[18].

El análisis del DIAOC permite una valoración positiva en otros aspectos, en particular:

1) constituye una aproximación global, holística, a ese régimen normativo; 2) realiza un tratamiento diferenciado y específico de los aspectos relativos al *Ius ad bellum* y al *Ius in bello*; 3) supone un ejercicio de confirmación de la aplicación del derecho internacional a las operaciones en el ciberespacio y de afirmación de las competencias soberanas

[18] Siguiendo el informe preparado por el Comité Internacional de la Cruz Roja (CICR), «cyber tools and methods can proliferate in a unique manner, one that is difficult to control. Today, sophisticated cyber attacks are carried out only by the most advanced and best-resourced actors. But once a cyber tool has been used, stolen or leaked, or becomes available in some other way, actors other than those who developed it may be able to find it, reverse-engineer it, and repurpose it for their own —possibly malicious— end» (THE INTERNATIONAL COMMITTEE OF THE RED CROSS. *International humanitarian law and the challenges of contemporary armed conflicts*. Ginebra: 2019, p. 20).

propias dentro de ese marco jurídico; 4) contiene un posicionamiento claro sobre las distintas situaciones posibles, su calificación jurídica y las modalidades de respuesta prevista; y 5) se muestra especialmente crítico frente a la interpretación realizada en el manual de Tallin reconociendo su valor, pero situándolo en el terreno exclusivamente doctrinal porque es una iniciativa «de nature à stimuler la réflexion international»[19].

La política diseñada en el DIAOC se aparta expresamente de los contenidos del manual de Tallin, además de implícitamente en otros casos, en cuatro aspectos fundamentales: 1) la adopción de un criterio funcional para la calificación de una ciberoperación como un ataque, que permite incluir los supuestos en los que los efectos son disruptivos y no solo destructivos, en lugar de seguir los criterios materiales defendidos en el manual; 2) el rechazo a la interpretación extensiva de la legitima defensa en el caso de incumplimiento por parte de un Estado de su obligación de diligencia debida porque el no respeto de esa obligación no constituye una excepción al principio de prohibición del uso o amenaza de la fuerza y porque hay otras respuestas razonables y legítimas para hacer frente a esa situación; 3) la presunción de la naturaleza civil de un bien protegido por el principio de distinción en caso de duda, sin necesidad, como aconseja el manual, de realizar una nueva determinación sobre su naturaleza; y 4) la protección de los sistemas y los datos de contenido, de naturaleza civil, vinculados a bienes merecedores de una protección especial porque esa protección específica dispensada a los bienes es extensible a los sistemas y datos que garantizan su funcionamiento. No hay que olvidar que, en derecho internacional, el intérprete auténtico y primigenio de la norma es el Estado como sujeto principal de este ordenamiento jurídico. Por ello, el DIAOC está llamado a ser una referencia ineludible para otros Estados a nivel individual y en el marco de los trabajos del GEG y del OEWG. Solo cabe esperar que se corrijan sus carencias mientras se sigue avanzando en sus aspectos positivos.

*Margarita Robles Carrillo**
Profesora titular de Derecho Internacional Público y RR. II., Univ. Granada
Network Engineering & Security Group (NESG)

[19] DIAOC, p. 5.