Bermejo García, Romualdo / López-Jacoiste Díaz, Eugenia

La ciberseguridad a la luz del Jus ad Bellum *y del* Jus in Bello

Eunsa Pamplona, 2020, 223 pp.

Es indudable que uno de los retos actuales más importante en las relaciones internacionales es el de las amenazas que representa la ciberseguridad y las respuestas que a las mismas puede ofrecer el Derecho Internacional, especialmente desde los sectores del *Jus ad bellum* y del *Jus in bello*. En palabras de los autores de esta monografía, esta relación se ve muy clara si se parte «de la premisa de que es posible que ataques cibernéticos puedan pasar el umbral previsto en el artículo 2.4 de la Carta de las Naciones Unidas, y constituir ataques armados que den lugar al derecho de legítima defensa tanto consuetudinario como convencional, de conformidad con el artículo 51 de la Carta de las Naciones Unidas, siempre que el ataque reúna los requisitos previstos para poder ejercer ese derecho. Estos aspectos son los que queremos abordar».

Para abordar estos objetivos, tras unas palabras previas y una introducción, los autores presentan un capítulo titulado «El ciberespacio y las amenazas a la paz y a la seguridad internacionales. Posicionamientos adoptados por algunos Estados». En este capítulo, se parte de comentar la doble dimensión de las Estrategias de seguridad cibernética. En caso de amenazas o ataques cibernéticos, los Estados no sólo deben adoptar acciones defensivas para disuadir a los posibles agresores, sino también ofensivas. Por ejemplo, en estos casos se intentará adoptar en primer lugar medidas que consistirán en introducir en las redes medidas no ofensivas, como los denominados «*White worms*» para detectar las causas de la amenaza y combatir después el mal funcionamiento del sistema, es decir, el «*malware*». Pese a ello, puede ocurrir que las amenazas se repitan con cierta intensidad y de forma cada vez más grave. En estos casos, habrá que adoptar medidas más contundentes y ofensivas que permitan perseguir a los atacantes en sus propias redes con diversos fines como recuperar la información obtenida, borrar los datos robados o impedir su distribución, sin olvidar la eventual inutilización de la información robada, así como las redes, servidores, etc., que sean responsables del hostigamiento o de los ataques. Con estas premisas, los autores analizan las virtudes y lagunas de las diversas estrategias de ciberseguridad o de ciberdefensa con las que se han ido dotando con el tiempo la Unión Europea, Estados Unidos, Reino Unido, Francia, Alemania y España.

El siguiente capítulo está dedicado a la ciberdefensa en el marco del *Jus ad Bellum*. Los autores han estructurado este capítulo en tres epígrafes, en los que respectivamente se preguntan si podría considerarse los ciberataques como «ataques» en el sentido de la Carta de las Naciones Unidas y analizan tanto las operaciones cibernéticas y la legítima defensa, como los principios de necesidad y proporcionalidad en su ejercicio. Se parte de la premisa de que en el marco del *Jus ad Bellum*, las medidas que se adopten en el marco de la ciberdefensa tendrán que adecuarse al régimen jurídico internacional vigente que regula el uso de la fuerza armada, entre los que se encuentra el capítulo VII de la Carta de las Naciones Unidas y, en particular, el derecho a la legítima defensa, tal y como se contempla en el Derecho consuetudinario y en el artículo 51 de la Carta, que reconoce expresamente «el derecho inmanente de legítima defensa, individual o colectiva, en caso de ataque armado contra un miembro de las Naciones Unidas...». A ello se debe añadir que la legítima defensa requiere también el cumplimiento del principio de la necesidad y de la proporcionalidad.

El examen realizado, demuestra que en el ámbito de la ciberdefensa sí es posible considerar que determinados hechos sí caen en el ámbito de aplicación del artículo 2.4 de la

Carta. Los autores tienen bien presente que la Corte Internacional de Justicia señaló expresamente que las disposiciones de la Carta relativas al uso de la fuerza «se aplican a cualquier uso de la fuerza, sin importar las armas empleadas» (Opinión sobre la legalidad de la amenaza o uso de las armas nucleares). Los autores también tienen en cuenta que, para la Corte, sólo los ataques que revistan una cierta gravedad, son ataques armados (Actividades militares y paramilitares en y contra Nicaragua). Aunque reconocen que, en el ámbito de la ciberdefensa no siempre será fácil establecer el umbral a partir del cual el ataque pueda ser considerado como grave o no, defienden una interpretación amplia, al basarse sobre todo en las consecuencias del ataque, más que en el instrumento utilizado. Así, concluyen afirmando que las normas del *Jus ad Bellum* de la Carta se amoldan también a las amenazas y ataques del ciberespacio, al tener cierta flexibilidad que les permite aplicarse a medios y contextos no previsibles en la época de su redacción.

También en el caso de las operaciones cibernéticas y la legítima defensa, los autores reconocen que, a pesar de los problemas y especificidades que implican, pueden acarrear el derecho de legítima defensa, siempre que presenten las características requeridas por el Derecho internacional para que puedan ser considerados como «ataques armados» y que presenten una cierta gravedad. Defienden que para saber cuándo un ciberataque puede ser considera un ataque armado, depende de su escala y sus efectos. Sostienen que el criterio determinante es si los efectos o las consecuencias de la operación cibernética son equiparables a los que se hubieran producido con una acción calificable como ataque armado con armas tradicionales. Analizan algunas peculiaridades en la aplicación de la legítima defensa frente a los ciberataques, como la necesidad de existencia de un elemento transfronterizo, la «inminencia» del ataque cibernético para que pueda aplicarse la legítima defensa preventiva, la posibilidad de que estos ataques cibernéticos no sean realizados por Estados, etc. Finalmente, llegan a la misma conclusión en el análisis de los principios de necesidad y de proporcionalidad que han de respetarse en el ejercicio de la legítima defensa y de las peculiaridades que presenta su aplicación a los ciberataques.

En el tercer capítulo, titulado «Los ciberconflictos a la luz del *Jus in Bello*», los autores abordan el estudio de si, dadas las peculiaridades de este sector, se tienen que aplicar también los principios y reglas del Derecho Internacional Humanitario» aplicables a los conflictos armados. Los autores reconocen que la aplicación del Derecho Internacional Humanitario a las ciberoperaciones está ya hoy en día aceptado, a pesar de las especificidades que las operaciones cibernéticas encierran. Consideran evidente, y con razón, que el Derecho Internacional Humanitario se aplica a las ciberoperaciones durante los conflictos armados, por lo que el ciberespacio se considera un campo de guerra similar al terrestre, marítimo o aéreo, pues cuando se aprueban las normas del Derecho Internacional Humanitario, sean éstas convencionales o consuetudinarias, se hacen para regular los conflictos armados no sólo presentes, sino también futuros. Destacan en este sentido que la Corte Internacional de Justicia afirmó que las normas y principios del Derecho Internacional Humanitario aplicables en los conflictos armado rigen para todas las formas de guerra y todos los tipos de armas, incluyendo las del «futuro» (Opinión sobre la legalidad de la amenaza o uso de las armas nucleares).

Esta monografía concluye con un interesante capítulo, en el que se examina la aplicación de las reglas del Derecho Internacional Humanitario durante las hostilidades. De una manera muy sistemática y rigurosa, los autores estudian las operaciones cibernéticas y las normas que regulan las «nuevas armas», el principio de distinción, el principio de distinción y la cuestión de la participación de civiles en las hostilidades, el principio de proporcionalidad y el principio de precaución. Por lo que se refiere al primer aspecto, parten de la aplicación del artículo 36 del Protocolo Adi-

cional I que obliga a los Estados a examinar si el empleo de las «nuevas armas» quedaría prohibido en ciertos casos o en todas circunstancias. Apuntan, y con razón, que la efectividad de la cláusula *Martens* puede aportar los elementos de juicio necesarios para la valoración de la licitud o no de los ciberataques y bajo qué circunstancias.

Es bien conocido, además, que el principio de distinción es uno de los pilares más fundamentales del Derecho Internacional Humanitario, que comprende la de distinguir en todo momento «entre combatientes y población civil», así como entre «bienes de carácter civil» y «objetivos militares», pudiendo dirigir las operaciones militares sólo contra estos últimos. No obstante, lo que no es tan fácil es la distinción en el caso concreto de lo que son bienes de carácter civil y bienes militares. A ello los autores dedican varias páginas que resultan del máximo interés en el caso de los ciberataques.

También son sumamente interesantes y originales las reflexiones que los autores realizan acerca del principio de distinción y la cuestión de la participación de civiles en las hostilidades. Es obvio que los civiles gozan de protección durante las hostilidades, aunque ésta cesa cuando participan directamente en las mismas, ya que entonces pueden ser objeto de ataques cibernéticos o de cualquier otra índole. Los autores son partidarios de considerar que, tanto a los piratas informáticos, como a los grupos no militares que participan en las operaciones cibernéticas, se les puede calificar como «grupos armados organizados», es decir, civiles que sí participan en las hostilidades, cuando se cumplen los tres criterios acumulativos de intensidad del daño, causalidad directa y nexo de beligerancia. No obstante, señalan los muy numerosos problemas que pueden suscitarse en la práctica, ya que la identificación de los piratas informáticos es bastante más compleja que la de los combatientes civiles de las operaciones físicas tradicionales.

Respecto del principio de la proporcionalidad, los autores sostienen que la proporcionalidad siempre exige un examen objetivo de la situación que pueda conducir a seleccionar los medios de los que se disponga con el fin de evitar los daños colaterales excesivos en los ataques, incluidos los ataques en el ámbito cibernético. Esta evaluación tendrá obviamente ciertas dosis de relativismo y de subjetividad. Esta evaluación determinará la dosis de probabilidad de que los eventuales daños colaterales sean o no excesivos en relación con la ventaja militar que se quiere obtener. Esta operación se llevará a cabo pensando siempre en el resultado, es decir, la protección de la población civil, aunque esta evaluación servirá sólo para el caso en cuestión, y dependerá de las circunstancias. En consecuencia, el primer paso que se deberá realizar es verificar si los objetivos que se quiere atacar no son civiles, ni objetos civiles. Pero si los objetivos son militares (fuerzas armadas, civiles que participan directamente en las hostilidades u objetos militares), el ataque será legal y lícito, siempre y cuando, por supuesto, que no se prevea daños excesivos a la población civil en relación con lo que se quiere obtener como ventaja militar en un caso determinado.

Finalmente, analizan la aplicación del principio de precaución en el ámbito cibernético. Los autores parten de considerar que éste es un principio que pertenece al ámbito del Derecho consuetudinario, tanto en los conflictos armados internacionales, como en los no internacionales. El principio de precaución implica que se tengan que adoptar medidas antes de llevar a cabo los ataques, incluidos los cibernéticos, con el fin de proteger a la población civil y a los bienes civiles de los efectos que puedan generar las operaciones militares. Este criterio se aplica tanto a la parte atacante, que debe hacer todo lo que sea factible para evitar causar daños incidentales como resultado de sus operaciones, como a la parte que es atacada, la que, dentro de lo posible, deberá adoptar todas las medidas necesarias para proteger a la población civil bajo su control contra los efectos de los ataques enemigo. Los autores, no obstante, no dejan de analizar y señalar las peculiaridades que la

aplicación de este principio puede tener en los casos de ciberataques.

Debido a su documentado y riguroso estudio, la lectura de esta monografía se recomienda altamente, al ser sin duda alguna el mejor estudio en lengua española sobre la sumisión de la ciberseguridad a los mandatos del Derecho Internacional, especialmente desde la óptica del *Jus ad Bellum* y del *Jus in Bello*.

Valentín Bou Franch
Catedrático de Derecho Internacional Público
y Relaciones Internacionales
Universidad de Valencia

Morán Blanco, Sagrario

Lucha contra el narcotráfico en América Latina.
La labor de la Organización de Estados Americanos (OEA)

Prólogo de José Luís Soberanes Fernández, Tirant lo Blanc, Valencia, 2021, 384 pp.

El narcotráfico ha sido desde hace ya varias décadas un tema recurrente no solo en el ámbito latinoamericano y americano en general, sino también a nivel internacional. Sin embargo, no es fácil encontrar en nuestra disciplina estudios tan pormenorizados sobre una cuestión que tiene diversas ramificaciones que no son solo económicas, sino también políticas y sociales, como la obra que nos presenta la Profesora Sagrario Morán, en la que nos muestra con ciertas dosis de humildad sus profundos conocimientos del tema, a pesar de la complejidad que encierra, sin olvidar el papel desempeñado en esta esfera la Organización de los Estados Americanos. Como ya nos señala la autora en sus palabras previas, el narcotráfico en América Latina y el Caribe «es una de las principales manifestaciones del Crimen Organizado transnacional, y es la causa primordial de la inseguridad que se vive en la región». Es más, el prologuista de esta excelente obra pone el dedo en la llaga al indicar que: «La América Latina no es libre... pero desde hace tres décadas dos cánceres corroen el vigoroso cuerpo latinoamericano y caribeño: el crimen organizado y el Narcotráfico. Estos tiranos de mil rostros han arrebatado a los habitantes de estas tierras el derecho fundamental de vivir tranquilos y libres en sus propios hogares».

La estructura de la obra es cartesiana. Dividida en dos partes perfectamente equilibradas, y escrita con rigor y una lectura muy amena, uno se sorprende al ver la finura de los análisis que lleva a cabo la autora. En la primera parte, la Profesora Morán va desgranando con un hilo conductor lógico el complejo y complicado panorama sociopolítico en el crimen organizado y el Narcotráfico. Ambos conceptos van a la par, como si uno fuera corolario del otro. El análisis que lleva a cabo la autora le lleva primero a delimitar ambos conceptos, para pasar después a cómo históricamente se han ido combinando según las circunstancias. Desde esta perspectiva, la autora nos indica que es muy difícil definir con precisión el concepto de crimen organizado, pero sobre todo «aquilatar una noción detallada que sea aplicable por todos los Estados y Organizaciones internacionales» (p. 42). No obstante, sí que desgrana con sumo detalle una seria de características como son su carácter transnacional, una gran diversidad en sus manifestaciones, así como su capacidad para establecer alianzas y vínculos con diversas autoridades de los Estados en los que se desarrolla (pp. 37-43). Por otro lado, respecto al narcotráfico la autora lo considera como que es «la expresión primordial del Crimen Organizado en América Latina y el Caribe (pp. 43