PIERNAS LÓPEZ, J.J., *Ciberdiplomacia y Ciberdefensa en la Unión Europea*, Cizur Menor, Thomson Reuters Aranzadi, 2020, 203 pp.

No resulta sencillo tomar contacto con el ámbito material del Derecho internacional vinculado al ciberespacio. Ello se debe a distintos motivos, entre otros, su actualidad, el hecho de que se encuentre en pleno desarrollo y las especificidades que lo vinculan con otras disciplinas que poco se asemejan a las ciencias jurídicas y sociales, ya sea del ordenamiento jurídico internacional o del Derecho de la Unión Europea.

Por ello, la monografía que recensionamos tiene como principal virtud conseguir que la inmersión en el análisis que realiza su autor de la estrategia de respuesta de la Unión Europea a las amenazas provenientes del ciberespacio, sea clara y placentera, sin dejar de poner de relieve aspectos bien sensibles que aborda utilizando la normativa en materia de responsabilidad internacional o la vinculada al uso de la fuerza. El profesor Piernas López desgrana, así, de forma sistemática y prolijamente documentada los dos principales instrumentos con los que cuenta la Unión Europea para dicho cometido, la *ciberdiplomacia* y la *ciberdefensa*, protagonistas de su trabajo, que aborda desde una triple estructura, que describimos más abajo.

La lectura de esta monografía, aparentemente breve, se densifica y expande a medida que el autor avanza, sobre todo en la parte segunda y central de la obra -dedicada a la ciberdiplomacia y a la ciberdefensa, que consideremos de mayor interés- bien hilvanada con otros sectores. Una característica del trabajo del profesor Piernas López, no excesivamente común, es que permite que su lector pueda ser tanto un especialista en el ámbito sustantivo de la acción exterior de la Unión Europea (UE), conocedor del Derecho de la Unión y familiarizado con el Derecho internacional, como un estudiante de Grado o posgrado avispado que necesite comprender las bases jurídicas del Derecho internacional y europeo ante estos nuevos retos tecnológicos, así como la respuesta de la Unión. Nos encontramos, por tanto, con una obra versátil que resultará de utilidad a investigadores con perfiles y capacidades dispares, gracias a la claridad y al carácter lineal -excesivamente, en nuestra opinión, en el capítulo primero- con la que se ha redactado.

La primera de las tres partes de la monografía se ocupa de la política de ciberseguridad de la Unión Europea. Siendo la más descriptiva de la obra, esta parte realiza un necesario examen de los principales instrumentos con los que ha contado hasta el momento presente, vinculados en su inicio a la prevención de la ciberdelincuencia -presentes desde 2010 en la Estrategia de Seguridad Interior de la UE y en una Estrategia propia ya de ciberseguridad tres años después, revisada en 2017-, en el que la política de ciberseguridad se caracteriza, como señala su autor, por su carácter transversal, interno e internacional, incluyendo elementos de mercado interior, de Política Exterior y de Seguridad Común (PESC) y de Política Común de Seguridad y Defensa (PCSD). Esta parte primera finaliza colocando el despliegue de las redes 5G en el punto de mira normativo por las amenazas que plantea para la ciberseguridad, lo que requiere de un enfoque coordinado entre los Estados Miembros de la Unión y las instituciones europeas, incluyendo el mandato de la Agencia de la UE para la Ciberseguridad (ENISA).

REEI, núm. 41, junio 2021
DOI: 10.17103/reei.41.39

La parte nuclear y más sugerente de la monografía es claramente la segunda que, estructura en tres capítulos, destina los dos primeros a la *ciberdiplomocia de la UE*. En ellos examina, primero, sus orígenes y evolución hasta la adopción del Marco para una respuesta diplomática conjunta de la UE a las actividades informáticas malintencionadas (capítulo 2) y, segundo, el desarrollo evolutivo de las medidas de ciberdiplomacia y la adopción de medidas restrictivas frente a ciberataques (capítulo 3) -con base en una decisión y un reglamento, ambos de 2019- como régimen temático sancionador específico con el objeto de impedir y contrarrestar los ciberataques particularmente graves que constituyan una amenaza externa para la Unión o sus Estados miembros. Resulta de utilidad el esfuerzo delimitador conceptual que el autor realiza de la ciberdiplomacia, impulsada en 2015 y, sobre todo, dos años después con la adopción de distintos instrumentos por la creciente amenaza por ciberataques más destructivos y frecuentes. Resulta de especial interés el análisis más exhaustivo y las reflexiones que realiza el profesor Piernas López sobre la imputación de responsabilidad internacional a terceros Estados, cuando se adoptan medidas restrictivas (sanciones) por parte de la Unión basándose en la aplicación del Derecho internacional -incluyendo el consuetudinario-, así como la incardinación de dichas sanciones como medida de retorsión "desnaturalizada", que plantea dudas sobre su legitimidad.

El tratamiento de asuntos como el despliegue de la red 5G, los ciberataques WannaCry, NotPetya o los maquinados por el grupo denominado APT10 -responsable de la tentativa de ciberataque a la Organización para la Prohibición de Armas Químicas (OPAQ)- entre otros, aporta un valor añadido a la obra, si bien podría haber enriquecido y centrado aún más su atención en estas cuestiones prácticas que tan bien ilustran los contenidos teóricos; entre ellos, las sanciones adoptadas -por ejemplo, el 30 de julio de 2020- contra seis individuos y tres entidades de Rusia, Corea del Norte y China por parte del Consejo de la Unión que el autor examina. La vinculación y comparaciones con el Reglamento de diciembre de ese mismo año sobre medidas restrictivas contra violaciones y abusos graves de los derechos humanos, ya utilizado recientemente incluyendo a individuos que ostentan cargos y a entidades relacionadas con los terceros Estados arriba citados, junto a algunos otros, no constituyen una casualidad, sino un esfuerzo por parte de la UE, pese al carácter limitado de las medidas a adoptar -inmovilización de bienes y la prohibición de viajar a territorio de un Estado miembro de la Unión- de identificar a determinados Estados y remar en una misma dirección. Una UE que muestre algo de músculo para defender y promover los valores en los que se basa, incluyendo el ciberespacio.

El capítulo cuarto se centra en la evolución hacia una política de *ciberdefensa* de la UE, exponiendo el autor la necesidad de reforzarla sin incurrir en duplicidades con la OTAN. Destaca la minuciosidad del análisis sobre el fundamento jurídico adecuado a invocar en casos de ciberataques graves, bien la cláusula de solidaridad del art. 222 TFUE en caso de ataque terrorista o de "catástrofe cibernética", o bien la de defensa mutua del art. 42.7 TUE, en casos extremos, en este último, por ejemplo, cuando los ataques tengan como resultado la muerte o lesión de personas, causen daños físicos, destruyan bienes significativos o infraestructuras críticas. Las obligaciones que conlleva invocar una u otra cláusula, el ámbito territorial de aplicación, su atribución a actores no estatales o incluso la sensible utilización de la defensa mutua en caso de "ataque inminente" son abordados

DOI: 10.17103/reei.41.39

con solidez, sin olvidar los factores políticos y de oportunidad, que siempre entran en juego.

La parte tercera de la obra contiene un compendio en el que se recogen de forma sistemática las conclusiones principales a las que el autor ha llegado en cada uno de los capítulos comentados. Pese a su carácter reiterativo, resultan de utilidad para comprender el objetivo logrado de su autor.

En definitiva, nos encontramos ante una monografía coherentemente articulada, bien documentada y redactada con claridad. Ideal para para una inmersión jurídica exitosa en el ciberespacio a través de la Unión Europea y sus Estados miembros.

Carmela Pérez Bernárdez
Universidad de Granada

DOI: 10.17103/reei.41.39