ISSN: 2697-1631 | ISSN-e: 2697-2239

La cobertura de los ciberataques patrocinados por Estados en el derecho de seguros español

Ignacio Sánchez Gil

Doctorando en Derecho Mercantil.
Universidad Complutense de Madrid (España)
isanchez.gil98@gmail.com | https://orcid.org/0000-0003-0130-1350

Este trabajo ha obtenido el **1.er Premio «Estudios Financieros» 2023** en la modalidad de **Derecho Civil y Mercantil**.

El jurado ha estado compuesto por: don José Ramón Navarro Miranda, doña Marlen Estévez Sanz, doña Esther de Félix Parrondo, don Ramón Fernández Aceytuno Sáenz de Santamaría, doña Esther Muñiz Espada y don Pedro Portellano Díez.

Los trabajos se presentan con seudónimo y la selección se efectúa garantizando el anonimato de los autores.

Extracto

Desde mediados del siglo XX ha existido un rechazo generalizado por parte del sector asegurador hacia la cobertura de los daños derivados de conflictos armados. Los motivos principales radican en la teórica imprevisibilidad de estos sucesos, dificultando el desarrollo de modelos actuariales precisos; además de en su aptitud para provocar daños masivos en periodos de tiempo muy concentrados, lo que puede derivar en una presión desmedida sobre la solvencia de las aseguradoras. Como consecuencia, resulta común que ciertas pólizas exceptúen de su cobertura los daños provocados por conflictos armados. En los últimos años, determinados Estados han venido promoviendo ciberataques dirigidos contra objetivos externos como parte de sus estrategias geopolíticas. Esto ha suscitado el debate sobre la consideración de estos ataques como constitutivos de conflictos armados y, consecuentemente, sobre su cobertura por las aseguradoras. A lo largo del presente trabajo pretendemos analizar el tratamiento que los ciberataques patrocinados por Estados reciben en el derecho español, en el que, según discutiremos, la exclusión de los daños producidos por conflictos armados, y otros sucesos extraordinarios, tiene rango legal.

Palabras clave: seguros; ciberataque; guerra; conflicto armado; ciberguerra.

Recibido: 03-05-2022 / Aceptado: 08-09-2022 / Publicado: 05-10-2023

Cómo citar: Sánchez Gil, I. (2023). La cobertura de los ciberataques patrocinados por Estados en el derecho de seguros español. *CEFLegal. Revista Práctica de Derecho*, *273*, 5-42. https://doi.org/10.51302/ceflegal.2023.19019

The coverage of state-sponsored cyberatacks in Spanish insurance law

Ignacio Sánchez Gil

This paper has won the **1st Financial Studies 2023** Award in the category of **Civil and Commercial Law**.

The jury members were: Mr. José Ramón Navarro Miranda, Mrs. Marlen Estévez Sanz, Mrs. Esther de Félix Parrondo, Mr. Ramón Fernández Aceytuno Sáenz de Santamaría, Mrs. Esther Muñiz Espada and Mr. Pedro Portellano Díez.

The entries are submitted under a pseudonym and the selection process guarantees the anonymity of the authors.

Abstract

The insurance industry has generally rejected the coverage of damage arising from armed conflicts since the mid-twentieth century. The main reasons lie in the theoretical unpredictability of these events, making it difficult to develop accurate actuarial models, as well as in their ability to cause massive damage in very concentrated periods of time, which can lead to excessive pressure on the solvency of insurers. As a result, it is common for certain policies to exclude damage caused by armed conflicts. In recent years, certain States have been sponsoring cyber-attacks against foreign targets as part of their geopolitical strategies. This has given rise to the debate on the consideration of these attacks as constituting armed conflicts and, consequently, on their coverage by insurers. Throughout this paper, we intend to analyze the treatment that state-sponsored cyber-attacks receive in Spanish law, where, as we will discuss, the exclusion of damages caused by armed conflicts, and other extraordinary events, is included in a legal norm.

Keywords: insurance; cyberattack; war, armed conflict; cyberwar.

Received: 03-05-2022 / Accepted: 08-09-2022 / Published: 05-10-2023

Citation: Sánchez Gil, I. (2023). La cobertura de los ciberataques patrocinados por Estados en el derecho de seguros español. *CEFLegal. Revista Práctica de Derecho*, *273*, 5-42. https://doi.org/10.51302/ceflegal.2023.19019

Sumario

1. Introducción

El 27 de junio de 2017, un programa informático malicioso se propagó a través de equipos situados a lo largo de los cinco continentes a una velocidad que en aquel momento resultaba insólita. El *software* malicioso o *malware* –que se conocería posteriormente como NotPetya–[1] hacía uso de una vulnerabilidad en el sistema operativo Windows para acceder a un equipo, bloquearlo y esparcirse a otros sistemas dentro de la misma red (Greenberg, 2018). En un primer momento se creyó que NotPetya era un tipo de *ransomware*, esto es, un programa informático malicioso que cifra los datos de un equipo informático, y exige un desembolso a su titular (típicamente en forma de criptomoneda) para restaurar la disponibilidad de los archivos. Sin embargo, los escasos pagos que se efectuaron siguiendo las indicaciones que mostraban las pantallas de los equipos infectados no surtieron efecto ninguno (Greenberg, 2018). NotPetya no tenía una finalidad económica, se trataba de un *malware* puramente destructivo.

A lo largo de las semanas siguientes este terrorista sin pólvora y sin rostro se expandió a la velocidad del dato, provocando daños que excedían los 10.000 millones de dólares a escala global, valiéndole el calificativo del ciberataque más costoso de la historia (Banerjea, 2018). El desconcierto inicial ante la aparente inexistencia de una motivación económica fue tornándose en certeza sobre la persecución de un propósito de índole política: algunos indicios, como el especial ensañamiento de NotPetya con los equipos situados en territorio ucraniano (de los que se estima que un 10 % se vio afectado por el *software* malicioso); o la coincidencia temporal del lanzamiento de NotPetya con el aniversario de la promulgación de la constitución de Ucrania (Greenberg, 2018) alineaban los intereses geopolíticos de Rusia con los de los desarrolladores del *malware*. Estos indicios resultaron ser lo suficientemente sólidos como para que Estados Unidos, Reino Unido y Australia, entre otros Estados (Kovacs, 2018), atribuyesen públicamente a la inteligencia rusa el desarrollo y la difusión de NotPetya.

De entre los innumerables casos de infecciones de NotPetya, dos son particularmente interesantes para nuestro trabajo. Aquel fatídico 27 de junio, copias del código malicioso se expandieron desde sistemas ucranianos hasta corromper 40.000 equipos de la farma-

[1] La denominación de NotPetya proviene a su vez de la similitud de este *malware* con otro programa malicioso que habría sido difundido un año antes, el Petya. Por su parte, se cree que este nombre constituye una referencia a un arma nuclear empleada por las fuerzas armadas soviéticas en una película de James Bond (Scherschel, 2016).

céutica alemana Merck[2]; además de otros 24.000 ordenadores portátiles, y 1.700 servidores internos de Mondelēz, conglomerado estadounidense de la alimentación que ostenta la titularidad de marcas como Oreo, Milka o Toblerone (Greenberg, 2018). Las dos entidades habían suscritos pólizas que aseguraban los daños derivados de ciberataques, por lo que no tardaron en ponerse en contacto con sus respectivas aseguradoras para solicitar que se les indemnizasen los menoscabos sufridos a raíz de la infección del NotPetya, que superaban los 1.000 millones de dólares en el caso de Merck y los 100 millones en el de Mondelēz (Perlroth, 2019). Lo que en un primer momento parecía una predisposición favorable al pago se tornó en negativa al reconocimiento de la indemnización a la par que más Estados imputaban el ciberataque a las fuerzas armadas rusas (Perlroth, 2019). El motivo residía en dos cláusulas de contenido prácticamente idéntico previstas en ambas pólizas y que excluían los daños resultantes de ataques hostiles o belicosos provenientes de Estados soberanos[3].

Las discrepancias terminaron por judicializarse. Un tribunal de Nueva Jersey falló a favor de Merck al entender que los términos «acción hostil o belicosa» no podían referirse sino a formas «tradicionales» de violencia[4], entendiendo como tales las hostilidades llevadas a cabo en los cuatro primeros dominios de la guerra (tierra, mar, aire y espacio), pero no así en el quinto (el ciberespacio). Mondelēz, por su parte, terminó por alcanzar un acuerdo con su aseguradora por una cantidad que no ha trascendido de manera pública (Martin, 2022).

Lejos de ser un acontecimiento aislado, el NotPetya no es sino uno de tantos ciberataques llevados a cabo por un Estado para promover sus intereses geopolíticos[5]. Resulta común asociar la cibercriminalidad con grupos relativamente organizados que persiguen una finalidad económica, y siendo cierto que el ánimo de lucro sigue motivando un porcentaje sustancial de las actividades ilícitas llevadas a cabo en el entorno digital[6], la im-

---

[2] *Merck & Co., INC and International Indemnity, LTD., v. ACE American Insurance Company et al.* (Superior Court of New Jersey, UNN L 002682-18). https://www.bloomberglaw.com/public/desktop/document/MerckCoIncvsAceAmericanInsuranCeDocketNoL00268218NJSuperCtLawDivA/1?doc_id=X1Q6O0S1OD82

[3] La redacción de la cláusula contenida en la póliza de Merck, que coincide sustancialmente con la de Mondelēz, excluía los daños dimanantes de: «acciones hostiles o belicosas (*warlike*) en tiempo de paz o de guerra, incluida la acción de obstaculizar, combatir o defenderse contra un ataque real, inminente o esperado por parte de cualquier (i) gobierno o poder soberano (*de iure* o *de facto*); (ii) fuerza militar, naval o aérea; o (iii) agente o autoridad de cualquiera de las partes especificadas en los puntos i o ii anteriores» (*Merck & Co., INC and International Indemnity, LTD., v. ACE American Insurance Company et al.*, p. 3).

[4] *Merck & Co., INC and International Indemnity, LTD., v. ACE American Insurance Company et al.*, pp. 10-11. La resolución a la que nos referimos ha sido recurrida, no existiendo en el momento de redacción del presente trabajo pronunciamiento del tribunal *ad quem*.

[5] A lo largo del presente trabajo, manejaremos una definición relativamente amplia de ciberataque, que comprenda toda actividad maliciosa tendente a recopilar, interrumpir, denigrar, degradar o destruir recursos de un sistema informático, o de la información (National Institute of Standards and Technology, 2019).

[6] De acuerdo con ENISA (Agencia Europea de Ciberseguridad), la principal motivación detrás de la mayoría de los ciberataques es la económica, seguida de cerca por la persecución de intereses geopolíticos (ENISA, 2022, p. 20).

portancia de los comúnmente conocidos como «ciberataques patrocinados por Estados» que persiguen intereses políticos no resulta en absoluto desdeñable[7]. A lo largo de las próximas páginas haremos uso del término de ciberataque patrocinado por un Estado para incluir tanto aquellos ataques llevados a cabo por grupos integrados en la estructura de un Estado, ejerciendo alguna forma de potestad pública (normalmente a través de sus fuerzas armadas o servicios de inteligencia); como a los ataques realizados por los denominados *proxies*, esto es, grupos que, sin representar *de iure* a un Estado, actúan bajo su dirección, ya sea a cambio de una contraprestación económica (cibermercenarios), o por una motivación ideológica.

Durante los últimos años se ha podido atestiguar un incremento drástico en la frecuencia y sofisticación de ataques patrocinados por Estados. La diversidad en la tipología de estos ciberataques patrocinados por Estados es tan amplia como lo permitan las posibles combinaciones de ceros y unos que componen el código subyacente y como lo requieran los intereses de los Estados patrocinadores. Esta heterogeneidad se vuelve manifiesta al estudiar las divergencias entre los medios y fines de los cuatro Estados más activos en lo que al patrocinio de ciberataques se refiere: China, Rusia, Irán y Corea del Norte[8]. China ha venido haciendo uso de incursiones a través del ciberespacio para llevar a cabo principalmente actividades de espionaje (Schwindt *et al.*, 2019, pp. 29 y ss.) tendentes a contribuir a sus esfuerzos para obtener la hegemonía tecnológica a nivel internacional, dirigidas tanto contra gobiernos extranjeros como contra empresas privadas (Microsoft, 2022, pp. 45 y ss.). También Rusia e Irán han recurrido a herramientas de ciberespionaje en los últimos años, si bien la diferencia principal con China radica en que estos regímenes han empleado de manera más habitual ataques con una finalidad netamente destructiva, cuyo objetivo es bloquear sistemas informáticos o, directamente, hacerlos inservibles[9]. En particular, Rusia ha dirigido múltiples ataques contra los gobiernos y las infraestructuras críticas de sus Estados vecinos (Georgia, Estonia y, especialmente, Ucrania) (Schwindt *et al.*, 2019, p. 9.), para así debilitar el funcionamiento de sus instituciones y crear una sensación de temor y caos en la población que, en último término, debilite la confianza en sus gobernantes (ENISA, 2022, pp. 25 y 26). Durante la invasión rusa a Ucrania en 2022, las operaciones

7 El Centro Criptológico Nacional considera los ataques patrocinados por Estados como el tipo de ciberamenaza más peligroso para nuestro país (Centro Criptológico Nacional, 2021, p. 7).

8 El Cyber Operations Tracker, base de datos gestionada por el Council on Foreign Relations (*think tank* estadounidense que registra ataques patrocinados por Estados que han trascendido de manera pública) imputa 222 ataques a China, 142 a Rusia, 84 a Irán y 62 a Corea del Norte. En un quinto puesto se encontraría Estados Unidos, con 18 ataques (Council on Foreign Relations, s. f.).

9 El caso iraní ejemplifica de manera paradigmática la relación que existe entre los intereses estratégicos de un Estado y sus campañas de ciberataques. Hasta 2015, grupos iraníes se ensañaron particularmente con instituciones financieras estadounidenses. La firma del Plan de Acción Conjunto (JPA) entre Irán y los miembros permanentes del Consejo de Seguridad de la ONU coincidió con un cese súbito en los ataques iraníes con objetivo estadounidense (Schwindt et al., 2019, p. 41). No obstante, los ataques se reintensificaron en 2021, a raíz del cambio de régimen en Irán (Microsoft, 2022, p. 47).

en el espacio cibernético se han empleado como un complemento a las hostilidades en el terreno físico, lo que explica que en el último año los ciberataques provenientes de Rusia y sus grupos afines hayan aumentado drásticamente, tanto en número como en potencial destructivo (Microsoft, 2022, p. 42). El ejército de Corea del Norte, además de atacar a sus rivales geopolíticos, como Estados Unidos o Corea del Sur (Schwindt *et al.*, 2019, pp. 45-47), presenta la peculiaridad de haber recurrido a la cibercriminalidad como una vía para obtener financiación. Así, se estima que, a lo largo de los últimos años, Corea del Norte habría recaudado más de 2.000 millones de dólares a través de campañas de ciberataques, habiendo destinado esos fondos a sufragar su programa nuclear[10].

Como se puede ver, el entorno digital se presenta como una vía eficaz para que los Estados persigan los objetivos de sus respectivas agendas, a un coste relativamente bajo (Lilly y Cheravitch, 2020, p. 10), y lo que es más importante, disminuyendo de forma significativa el riesgo de que se descubra la verdadera autoría del ataque. Para esto último, según decíamos antes, resulta especialmente útil el uso de grupos que no se encuadran *de iure* dentro de la estructura estatal o *proxies*[11] (cuya vinculación con el Estado resulta, en muchas ocasiones, prácticamente indemostrable, dificultando así la imputación a este de las actuaciones de aquellos). Existen casos en los que la relación entre Estado y *proxy* resulta más o menos evidente, ya sea por la coincidencia entre los intereses del Estado y las actuaciones del grupo, o por las conexiones entre miembros del *proxy* y representantes estatales[12]. Sin embargo, no son pocas las ocasiones en las que este vínculo se difumina. Conti fue uno de los grupos especializados en *ransomware* más importantes de los últimos años, hasta el punto de llevar al gobierno estadounidense a ofrecer una recompensa de hasta 10 millones de dólares a cambio de información sobre sus integrantes. Si bien se sabía que el grupo estaba alojado en Rusia, y que sus objetivos principales eran infraestructuras críticas de países mayoritariamente occidentales, se creía que actuaba persiguiendo fines exclusivamente económicos[13]. No obstante, en 2022 se hicieron públicas conversaciones

[10] Véase el Informe S/2020/151, elaborado por el Panel de Expertos del Consejo de Seguridad de la ONU, establecido de acuerdo con la resolución 1874 (2009), párrafos 57 y ss. https://www.securitycouncilreport.org/atf/cf/%7b65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7d/S_2020_151.pdf

[11] Esto no quiere decir que, en paralelo al recurso a *proxies*, los Estados no hayan desarrollado las capacidades técnicas de sus fuerzas armadas y servicios de inteligencia. Este ha sido el caso de Rusia, que, a lo largo de la última década, ha venido dotando de una mayor importancia a los perfiles técnicos dentro de sus estructuras internas, como evidencia el nombramiento de un académico especializado en ciencia computacional como subdirector del GRU, principal servicio de inteligencia ruso, en 2015 (Lilly y Cheravitch, 2020, p. 145).

[12] Un ejemplo sería el Ashiyane Digital Security Team, grupo contratado en múltiples ocasiones por la milicia iraní para llevar a cabo ciberataques (Insikt Group, 2019).

[13] Normalmente Conti cifraba los archivos (incluyendo información confidencial) de sus objetivos y exigía un rescate a cambio de desbloquearlos, y de no hacer la información pública. En la medida en que las actividades de Conti beneficiaban al gobierno ruso, sus integrantes no eran perseguidos activamente, pero no se conocía la existencia de una relación formal entre Rusia y el grupo (Peralta, 2022).

entre miembros de la inteligencia rusa y representantes de Conti que evidenciaban injerencias gubernamentales en la determinación de los objetivos del grupo (ENISA, 2022, p. 35).

El panorama dibujado por los ciberataques patrocinados es uno de hostilidades continuadas entre Estados, que en muchas ocasiones recurren a grupos interpuestos cuyo grado real de autonomía es un misterio. Esta situación se sitúa a medio camino entre las categorías paradigmáticas empleadas por los instrumentos de derecho internacional público que lidian con la violencia interestatal (guerra o conflicto armado)[14] y las meras actuaciones terroristas efectuadas por grupos motivados políticamente. No obstante, la cuestión sobre el encaje de la ciberviolencia dentro de las categorías clásicas de hostilidades interestatales no se puede circunscribir en exclusiva al derecho internacional público, en la medida en que existen normas legales y convencionales de naturaleza jurídico-privada que también atribuyen significación jurídica a estos conceptos.

Dentro del campo del derecho de los seguros existe una clara reticencia, especialmente pronunciada a raíz de la segunda mitad del siglo XX[15], hacia la cobertura de los daños producidos por eventos bélicos y similares[16]. Ello se justifica por el potencial de estos sucesos para producir daños colosales en periodos muy concentrados de tiempo, lo que puede generar una presión desmesurada sobre el sistema asegurador en su conjunto; además de su baja frecuencia y relativa imprevisibilidad, con lo que resulta muy complejo desarrollar modelos actuariales que estimen de forma precisa el potencial de los daños y, consecuentemente, el importe de las primas necesarias para cubrir el riesgo (OECD, 2021, p. 7). La yuxtaposición de estos factores explica que, por un lado, sea relativamente común que los daños producidos por conflictos armados y otros eventos similares se excluyan de manera expresa de la cobertura de las pólizas y, por otro, que en muchos sistemas legales se desarrollen sistemas públicos de aseguramiento que compensen el vacío que dejan las aseguradoras privadas (OECD, 2021).

---

[14] Han sido muchos los esfuerzos académicos dedicados a determinar si, y bajo qué circunstancias, un ciberataque podía constituir un recurso al uso de la fuerza, un ataque armado o, incluso, un conflicto armado. El documento más exhaustivo publicado al respecto en la fecha de redacción del presente trabajo es el conocido como «Manual de Tallín», publicado en 2013 por el Centro de Excelencia en Defensa Cibernética Cooperativa de la OTAN, disponible en https://www.onlinelibrary.iihl.org/wp-content/uploads/2021/05/2017-Tallinn-Manual-2.0.pdf

[15] En 1938, considerando los daños catastróficos causados por la Guerra Civil española, la Lloyd's Underwriters Association y la Association of British Insurers llegaron a un acuerdo para excluir los eventos bélicos de la cobertura de las pólizas de seguros emitidas en el Lloyd's of London (con la excepción de los seguros *marine*), mediante la cláusula conocida como NMA 464 (Cooper, 2022). Dicha cláusula fue adoptada como un estándar a nivel internacional, hasta los atentados del 11 de septiembre de 2001, que propiciaron la exclusión de los daños producidos por actos terroristas, juntamente por los ocasionados por eventos bélicos (Caamaño Malagón, 2022).

[16] Quizás la principal excepción serían los seguros de transporte internacional de mercancías (los seguros *marine*), en los que la cobertura de los eventos bélicos sigue siendo relativamente común (Caamaño Malagón, 2022).

La exclusión de eventos bélicos y belicosos ha dado lugar a un gran número de disputas a nivel internacional, relativas su extensión y límites[17], siendo las contiendas de Merck y Mondelēz las últimas representantes. A lo largo de las próximas páginas llevaremos a cabo un análisis sobre el tratamiento de esta cuestión en el derecho español, tratando de esbozar las circunstancias que podrían determinar que un ciberataque patrocinado por un Estado quede cubierto por una póliza privada, sea indemnizado por el consorcio de compensación de seguros (entidad pública que en España asegura determinados eventos extraordinarios) o no sea resarcible por ninguno de los dos. La relevancia de esta cuestión es manifiesta a la luz del notable incremento en los ataques patrocinados por Estados, además de la proliferación de pólizas de seguros que cubren los costes derivados de un ciberataque[18], que en los últimos años han atravesado un proceso de democratización, pasando de ser un producto exclusivo para clientes dotados de una relativa sofisticación tecnológica, a ser suscrito por entidades de dimensión más reducida (Giménez, 2020).

A tal fin, nos centraremos primeramente en examinar la consideración de un ciberataque patrocinado como un evento extraordinario, lo que condicionará su cobertura por parte de la aseguradora privada, o del consorcio de compensación de seguros. Aclarado lo anterior, analizaremos la posibilidad de la aplicación de la exclusión legal que en nuestro sistema se prevé para los daños producidos a consecuencia de conflictos armados.

2. Ciberataques patrocinados como eventos extraordinarios

2.1. El aseguramiento de los riesgos extraordinarios en el derecho español

El modelo español de cobertura de eventos bélicos y demás sucesos catastróficos se caracteriza por el papel preponderante del sector público. En este sentido, el primer párrafo

[17] Un resumen de los principales pronunciamientos jurisdiccionales al respecto en Estados Unidos puede encontrarse en Wolff (2022).

[18] Los daños producidos por un ciberataque pueden cubrirse por una póliza genérica, que no lidie de forma particular con los ciberriesgos, pero que no los excluya de manera expresa (por ejemplo, un contrato de seguro que cubra toda forma de lucro cesante), o por una póliza que lidie de manera expresa con los daños derivados de un ciberataque (los denominados ciberseguros). El origen de estos últimos se remonta al inicio del milenio y, más concretamente, a la progresiva aprobación de normas que venían exigiendo que las entidades que tratan datos personales notifiquen a las autoridades o a los interesados en caso de que se vean afectados por un ataque que comprometa sus datos (Jimeno Muñoz, 2019, p. 149). Las pólizas de ciberseguros pueden cubrir los daños en el *software* o *hardware* de los equipos afectados, los costes de recuperación del servicio, la pérdida de beneficio derivada de la paralización de la actividad, los costes de notificaciones exigidos *ex lege* e, incluso, el importe de los «rescates» pagados a los criminales en ataques de *ransomware* (Jimeno Muñoz, 2019, p. 249), si bien la industria es cada vez más proclive a extender la cobertura por este último concepto.

del artículo 44 de la Ley 50/1980, de contrato de seguro (LCS) dispone expresamente que «el asegurador no cubre los daños por hechos derivados de conflictos armados, haya precedido o no declaración oficial de guerra, ni los derivados de riesgos extraordinarios sobre las personas y los bienes, salvo pacto en contrario». Esta exclusión que, lejos de ser novedosa, entronca con la tradición de nuestro derecho[19], no aparecía en el texto original del proyecto de la LCS, sino que se introdujo a través de dos enmiendas presentadas durante la tramitación parlamentaria de la norma (Sánchez Calero, 2010, p. 983). *Prima facie*, se observa cómo la norma diferencia entre dos clases de daños que quedan excluidos: los que resulten de la materialización de riesgos extraordinarios, por un lado, y los que sean consecuencia de conflictos armados, por otro. Ninguno de los dos conceptos aparece definido en el texto legal. Adicionalmente, el final del precepto nos indica que la exclusión no tiene carácter imperativo; así, el asegurador sí que respondería por los daños referidos siempre y cuando así se disponga en el contrato.

La ausencia del aseguramiento privado se suple en parte por la función que lleva a cabo el sector público, y que se instrumentaliza a través del Consorcio de Compensación de Seguros (CCS)[20]. El CCS es una entidad pública empresarial, adscrita actualmente al Ministerio de Asuntos Económicos y Transformación Digital, y que desempeña, entre otras, funciones relativas al seguro agrario combinado, al seguro obligatorio de automóviles, a la liquidación de entidades aseguradoras y al aseguramiento de riesgos extraordinarios[21]. Para comprender de forma adecuada la significación del CCS resulta imprescindible referirnos, siquiera de manera sucinta, a la historia de la institución.

En 1941, los estragos ocasionados por la Guerra Civil española derivaron en disputas sobre su causa (motín o guerra), lo que resultaba determinante a la hora de decidir sobre su cobertura por parte de las pólizas privadas. La solución que se terminó implementando fue una de compromiso por la cual el Estado adelantaría parte del importe del que teóricamente eran deudoras las entidades privadas. El importe de los daños asegurados que excedía de dicha cantidad fue aportado por el Estado, a través de la emisión de deuda suscrita por las propias aseguradoras. Para amortizar esta deuda, se establecieron recargos obligatorios sobre las primas de seguro de diferentes ramos, que fueron recaudados por las aseguradoras (García Barona, 1997, pp. 403- 404)[22], encomendándose la administración

[19] Como señala Tirado Suárez (1995, p. 3774), el antiguo artículo 396 de nuestro Código de Comercio, en materia del seguro de incendios, excluía de la responsabilidad del asegurador aquellos daños ocasionados por fuerzas militares en contextos bélicos, así como aquellos derivados de tumultos populares.

[20] A nivel internacional, la intervención pública en la cobertura de los riesgos extraordinarios es enormemente común. No obstante, el modelo español destaca por el monopolio *de facto* que ostenta el CCS (OECD, 2021, pp. 20 y ss.).

[21] Véanse los artículos 6 y siguientes del Real Decreto Legislativo 7/2004, por el que se aprueba el texto refundido del Estatuto Legal del Consorcio de Compensación de Seguros.

[22] Sobre las normas jurídicas creadas como respuesta a las incertidumbres sobre la cobertura de los daños causados por la Guerra Civil, véase Hernando de Larramendi y Caballero García (1972, pp. 13 y ss.).

de estos fondos a tres instituciones públicas que se establecieron con carácter temporal: el Consorcio de Compensación de Riesgos de Motín, el Consorcio de Compensación de Accidentes Individuales y el Consorcio de Seguros Ramo Vida (Bonhome González, 2010, pp. 213-214). Si bien la cobertura pública de los riesgos catastróficos se instauró como una solución *ad hoc* para los daños acaecidos durante la Guerra Civil, este mismo sistema siguió operando de forma proactiva, extendiéndose su cobertura a los daños ocasionados en el siniestro de Santander de 1941, y en las catástrofes de Camfranc y Cádiz, en 1944 (Tirado Suárez, 1995, p. 3.775). A través de la Ley de 16 de diciembre de 1954, el Consorcio de Riesgos de Motín y el de Compensación de Accidentes Individuales se integrarían en el CCS, establecido con carácter permanente para la cobertura de los riesgos extraordinarios que afectasen a personas o cosas aseguradas en virtud de una póliza privada, que cubriría, pues, los riesgos «no extraordinarios»[23].

La cobertura del CCS se extendía a los daños originados por determinados sucesos de carácter extraordinario, incluyendo tanto fenómenos de origen natural (inundaciones, erupciones volcánicas, huracanes, etc.) como de origen humano (motines, alborotos, tumultos populares, etc.)[24]. Los daños producidos por conflictos armados quedaban excluidos en los ramos de cosas en virtud del artículo 5 b) de la Ley de 1954.

Inicialmente, la financiación del CCS provenía de un recargo obligatorio establecido *ex lege* sobre las primas comerciales derivadas de las pólizas privadas. No obstante, dicho sistema cambió a raíz del acceso de España a las Comunidades Europeas: el monopolio del consorcio sobre la cobertura de los riesgos extraordinarios, financiado mediante un recargo que tenía la naturaleza de prima obligatoria, parecía colisionar con las exigencias de liberalización del derecho europeo. Sin embargo, el relevante papel del consorcio dentro del ecosistema español no propiciaba una desaparición radical del mismo. Finalmente, con la aprobación de la Directiva 88/357/CEE, y su posterior transposición mediante la Ley 21/1990[25], se alcanzó una solución intermedia: se permitió que la iniciativa privada concu-

[23] Siendo cierto que la Ley de 16 de diciembre de 1954, sobre refundición de los Consorcios de Compensación de Riesgos Catastróficos sobre las Cosas y de Accidente Individuales en un solo «consorcio de compensación de seguros», e integrando en el mismo los seguros agrícolas, forestales y pecuarios, dotaba al consorcio de una vocación de permanencia, también se debe reconocer que la norma eludía la aceptación sin reservas del carácter permanente del CCS, afirmando que la institución se crea «sin perjuicio de que cuando la experiencia lo aconseje sean cubiertos por el Seguro privado los riesgos que ahora asume dicho Consorcio».

[24] La enumeración completa de los riesgos objeto de cobertura por el CCS se encontraba inicialmente en el artículo 8 del Decreto de 13 de abril de 1956, cuyo artículo 6 impedía que se asegurasen dichos riesgos mediante póliza privada.

[25] Ley 21/1990, de 19 de diciembre, para adaptar el Derecho español a la Directiva 88/357/CEE, sobre libertad de servicios en seguros distintos al de vida, y de actualización de la legislación de seguros privados. A través de esta norma, de carácter heterogéneo, se adecuan distintos preceptos relativos a la regulación del seguro a las exigencias europeas, y se dota de un nuevo estatuto legal al CCS, entre otros puntos.

rriese con el CCS en el aseguramiento de los riesgos extraordinarios, terminando con su carácter monopolístico. A pesar de ello, el recargo obligatorio se mantuvo, pero ya no como una prima de seguro, sino como un ingreso de naturaleza pública[26].

Aunque el monopolio sobre la cobertura de los riesgos extraordinarios hubiese desaparecido *de iure*, en la práctica el CCS sigue siendo el actor más relevante, por no decir el único[27], en lo que atañe al aseguramiento de los riesgos catastróficos. Tanto es así que la pretendida liberalización se ha tildado de «más ficticia que real» (Barrero Rodríguez, 2000, p. 223), ya que, aun cuando una póliza privada cubra los daños derivados de riesgos extraordinarios (en cuyo caso será la aseguradora privada, y no el CCS quien indemnice tales daños), el recargo obligatorio al CCS debe seguir satisfaciéndose. En otras palabras, la obligación de pagar el recargo del CCS es independiente de la cobertura del riesgo extraordinario en una póliza privada, por lo que no existe incentivo ninguno en pagar una sobreprima al asegurador privado para que cubra un riesgo ya cubierto por el CCS[28].

Desde la aprobación de la Ley 21/1990, y hasta la fecha de elaboración del presente trabajo, las innovaciones normativas más relevantes en lo que atañe al aseguramiento de los riesgos extraordinarios en España se producen en el año 2004 mediante la aprobación de un nuevo estatuto legal del CCS (TRECCS)[29] y del Reglamento del seguro de riesgos extraordinarios (RSRE)[30]. Son estas normas, juntamente con la LCS, las que esbozan los principales elementos del sistema español de aseguramiento de riesgos catastróficos.

---

[26] El carácter parafiscal del recargo obligatorio no contrariaba las exigencias del derecho europeo en virtud del artículo 25 de la Directiva 88/357/CEE, según la cual «todo contrato de seguro celebrado en régimen de prestación de servicios estará exclusivamente sometido a los impuestos indirectos y a las exacciones parafiscales que graven las primas de seguros en el Estado miembro en que se sitúa el riesgo […], así como, por lo que respecta a España, a los recargos legalmente establecidos en favor del organismo español "Consorcio de Compensación de Seguros"…». Esta salvedad a favor del CCS seguiría apareciendo en ulteriores normas europeas en materia de seguros, hasta llegar a la Directiva 2009/138/CE (Solvencia II), en su artículo 157.

[27] Véase OECD (2021, p. 23, nota 17).

[28] Los motivos a favor del mantenimiento del sistema actual se basan, principalmente, en la defensa de la solidaridad interterritorial en España. Dada la asimetría en la exposición a eventos catastróficos a través de nuestro territorio nacional (así, la experiencia empírica demostraría que los atentados terroristas habrían estado desproporcionadamente concentrados en el País Vasco; mientras que las catástrofes naturales harían lo propio en el área del Levante [García Barona, 1997, p. 412]). Justifican estos autores que, en caso de darse una liberalización plena, el coste del aseguramiento de la cobertura de los riesgos catastróficos sería asumido de forma mayoritaria por los territorios que están especialmente expuestos a los mismos.

[29] Real Decreto Legislativo 7/2004, por el que se aprueba el texto refundido del Estatuto Legal del Consorcio de Compensación de Seguros.

[30] Real Decreto 300/2004, de 20 de febrero, por el que se aprueba el Reglamento del seguro de riesgos extraordinarios.

2.2. Sucesos cubiertos por el CCS

El panorama actual, pues, se caracteriza por la ausencia de una prohibición expresa de aseguramiento de los riesgos catastróficos a través de pólizas privadas. En el infrecuente caso de que una aseguradora privada se obligue a indemnizar los daños producidos por eventos extraordinarios, la cobertura será asumida por dicha entidad en virtud de un contrato de seguro perfectamente lícito, y el CCS no se comprometerá de modo ninguno (siempre que la aseguradora no se haya declarado en concurso, ni esté sujeta a un procedimiento de liquidación)[31]. No obstante, será mucho más frecuente que sea el CCS quien responda por los daños resultantes de los riesgos catastróficos.

El requisito fundamental para que el consorcio asuma la cobertura de los riesgos extraordinarios sobre determinados bienes o personas es que los mismos se encuentren asegurados en lo que respecta a los riesgos ordinarios, de acuerdo con el llamado principio de complementariedad adhesiva. El CCS opera como una suerte de «asegurador complementario»[32], ya que su cobertura se condiciona a la existencia de un contrato de seguro cuyo objeto sean determinados riesgos ordinarios[33]. Dado este contrato, el asegurador privado responderá por los daños causados por eventos ordinarios, mientras que el CCS hará lo propio con los derivados de sucesos extraordinarios.

La retribución del CCS proviene de los recargos obligatorios que los asegurados deben satisfacer al abonar las primas de sus pólizas para la cobertura de riesgos ordinarios. Precisamente por ello, el asegurado que no se encuentre al corriente del pago de la prima pierde su derecho a la cobertura del consorcio. Los recargos son recaudados por las aseguradoras privadas por cuenta del CCS (percibiendo por ello una comisión de cobro, *ex* art. 18.5 del TRECCS). Como ya vimos, hasta la aprobación de la Ley 21/1990 estos recargos tenían la auténtica consideración de primas de un contrato de seguro. A partir de entonces, pasan a categorizarse como una forma de ingreso de derecho público de carácter no tributario[34].

---

31 Véase, a este respecto, el artículo 8.1 b) del TRECCS. Adicionalmente, resulta razonable pensar que, en aquellas situaciones en las que se asegure mediante una póliza privada el riesgo extraordinario en condiciones menos favorables para el asegurado que las que disfrutaría en caso de cobertura por el CCS, este último seguirá asumiendo los daños producidos por eventos catastróficos. En este mismo sentido se pronuncia Gonzalez de Frutos (1993, pp. 9-10).

32 Véanse las SSTS núm. 4343/1991, de 22 de julio, y núm. 4762/1996, de 9 de septiembre.

33 Y solamente riesgos ordinarios, ya que la cobertura de riesgos extraordinarios por el asegurador privado excluye la cobertura del CCS.

34 En este sentido, González de Frutos (1993, pp. 5 y ss.). El carácter no tributario se puede inferir de la redacción del TRECCS, cuyo artículo 23.1 enumera los recursos económicos del consorcio. Posteriormente, el artículo 23.4 establece que «el recargo destinado a financiar las funciones de liquidación de entidades aseguradoras es un tributo que grava los contratos de seguro», detallándose a continuación el hecho imponible, sujeto pasivo, etc. *Sensu contrario*, se deduce que el resto de los recargos a favor del CCS no tienen naturaleza tributaria.

No todo contrato de seguro determina la existencia de la cobertura del CCS. Al contrario, esta solo se produce en caso de que la póliza pueda encuadrarse dentro de algunos ramos a los que se refiere el artículo 7 del TRECCS[35]. En este caso, el texto de la póliza deberá incluir, de acuerdo con el artículo 8.3 de la misma norma, una cláusula en la que se haga referencia a la cobertura de los riesgos extraordinarios por parte del CCS[36].

Ratione loci, el aseguramiento por parte del CCS se condiciona a que el riesgo cubierto a través de la póliza se encuentre situado en España, conforme a los criterios enumerados en el artículo 6.2 del TRECCS[37].

Concurriendo los requisitos anteriores, y transcurrido el plazo de carencia (como regla general, de siete días naturales), el interés quedará asegurado ante los sucesos extraordinarios enumerados en el artículo 6.1 del TRECCS. Para que se reconozca el derecho a la indemnización, este suceso extraordinario deberá resultar en un daño directo sobre el interés asegurado. Estatuto y reglamento parecen circunscribir la resarcibilidad del daño a la existencia de un nexo de causalidad directa entre este y el suceso catastrófico, quedando excluidos los daños indirectos. Como excepción, el artículo 3 del RSRE prevé que, en determinadas circunstancias, y siempre que así se prevea mediante la póliza ordinaria, el consorcio indemnizará la pérdida de beneficios derivada de alguno de los acontecimientos catastróficos.

La pérdida de beneficios representa uno de los supuestos en los que el contenido de la póliza suscrita con la aseguradora privada afecta a la extensión de la cobertura por el CCS, pero no es el único. Esta cuestión enlaza con la pregunta sobre la concreta naturaleza de la relación que se establece entre consorcio y asegurado, y en qué medida se ve afectada por la póliza privada. La aprobación de la Ley 21/1990 (y el reconocimiento de la prima del CCS como ingreso de derecho público) suscitó un debate doctrinal entre aquellos que calificaban el vínculo entre consorcio y asegurado como una relación *ex lege*, condicionada

[35] Actualmente, se establece la obligatoriedad del recargo para los ramos de vida, en los contratos que garanticen exclusiva o principalmente el riesgo de fallecimiento, incluidos los que prevean, además, indemnizaciones pecuniarias por invalidez permanente o incapacidad temporal, en los términos y modalidades que reglamentariamente se determinen; el ramo de accidentes, en los contratos que garanticen el riesgo de fallecimiento o prevean indemnizaciones pecuniarias por invalidez permanente o incapacidad temporal; el de vehículos terrestres; vehículos ferroviarios; incendio y elementos naturales; otros daños a los bienes; y pérdidas pecuniarias diversas; así como las modalidades combinadas de estos, o cuando se contraten de forma complementaria; también el ramo de responsabilidad civil en vehículos terrestres automóviles.

[36] En la actualidad, el texto de dichas cláusulas se encuentra en la Resolución de 28 de marzo de 2018 de la Dirección General de Seguros y Fondos de Pensiones.

[37] Se considera que un riesgo se sitúa en España cuando afecta a: vehículos con matrícula española; bienes inmuebles situados en el territorio nacional; bienes muebles que se encuentren en un inmueble situado en España, estén o no cubiertos por la misma póliza de seguro, excepto aquellos que se encuentren en tránsito comercial; en el caso de seguros de personas, cuando el asegurado tenga su residencia habitual en España; y, en los demás casos, cuando el tomador del seguro tenga su residencia habitual en España o, si fuera una persona jurídica, tenga en España su domicilio social o la sucursal a que se refiere el contrato.

al perfeccionamiento de un contrato entre el asegurado y un asegurador privado (y que por lo tanto debería regirse exclusivamente por la normativa legal), y los que seguían apelando a la existencia de un auténtico contrato de seguro entre el CCS y el asegurado, nacido en virtud de la cláusula que debe incluirse obligatoriamente en el texto de la póliza ordinaria, y cuyo objeto serían los mismos intereses que los cubiertos por la aseguradora privada. La jurisprudencia se inclina por la segunda postura. En este sentido, la STS de 9 de septiembre de 1996[38] reconoció que entre CCS y asegurado surge un auténtico contrato de seguro autónomo, con la principal particularidad de que al mismo le serán de aplicación las normas especiales contenidas en su estatuto legal y, solo en su defecto, la LCS. Sin embargo, el Alto Tribunal matizó que la autonomía entre ambos contratos no alcanza el extremo de la total abstracción, ya que diversos elementos de la relación entre el CCS y el asegurado dependerán a su vez de la relación entre este último y la aseguradora privada[39].

Concurriendo los demás requisitos expuestos, el elemento clave para delimitar la cobertura de un daño por parte del CCS vis a vis con la aseguradora privada reside, pues, en su causa. En otras palabras, el hecho de que el daño se derive de un suceso extraordinario, o no, será el que determine si el mismo se encuadra en el ámbito de la póliza ordinaria, del contrato de seguro entre CCS y asegurado o en ninguno de los dos.

Los eventos extraordinarios se enumeran en el TRECCS y se definen en el RSRE[40]. Estatuto y reglamento cumplen, de esta forma, una doble función: por un lado, desarrollan el concepto de riesgo extraordinario del artículo 44.1 de la LCS, de cara a su no inclusión en las pólizas privadas, y por otro, delimitan los eventos que sí dan lugar a una indemnización por parte del consorcio.

---

38 STS núm. 4762/1996, de 9 de septiembre. La contienda que dio lugar a esta resolución se relaciona con los denominados «pactos de inclusión facultativa», esto es, determinadas cláusulas que se podían incluir en el contrato de seguro ordinario y que resultaban favorables para el asegurado. El CCS alegó que estas cláusulas le eran inoponibles, por no estar específicamente prevista en su normativa reguladora, tesis que terminó siendo rechazada por el Alto Tribunal. Este mismo criterio ha sido mantenido tras la aprobación del Estatuto y el Reglamento de 2004 (véase la SAP de Barcelona núm. 647/2012, de 5 de diciembre).

39 La cuestión de la oponibilidad de las cláusulas de inclusión facultativa quedó parcialmente zanjada mediante el artículo 5.2 del RSRE, que cita de manera expresa determinadas cláusulas que, de estar incluidas en la póliza ordinaria, vinculan al CCS. No obstante, sigue sin quedar claro si aquellas cláusulas que no aparecen en el RSRE les son o no oponibles al CCS.

40 Como recuerda la STS núm. 1102/1998, de 23 de noviembre, el desarrollo reglamentario del concepto legal de riesgos extraordinarios está sujeto al control de los tribunales, de tal forma que dicho desarrollo no puede resultar arbitrariamente restrictivo. Así, se afirma que «han de ser siempre los Tribunales […] los que han de decidir si la interpretación dada por la Administración al concepto jurídico indeterminado empleado por la norma con rango de ley se adapta a esta y agota su contenido o, por el contrario, la contradice por limitar expresamente su ámbito, excluyendo una parcela de la realidad a través del Reglamento, cuando dicha realidad está abarcada por la Ley». A la luz de la normativa actual, entendemos que dicho control solo podría extenderse a la definición de los acontecimientos catastróficos del RSRE, pero no así a la enumeración que efectúa el TRECCS, dado el rango de ley de este último (a menos que dicha enumeración hubiese excedido la delegación operada en su ley de bases).

La enumeración de los eventos catastróficos recoge un conjunto de supuestos heterogéneos, incluyendo fenómenos de origen natural (terremotos, maremotos, inundaciones extraordinarias, erupciones volcánicas, tempestad ciclónica atípica y caídas de cuerpos siderales y aerolitos), así como sucesos derivados de la acción humana (terrorismo, motín, tumulto popular, hechos y actuaciones de las Fuerzas Armadas o de las Fuerzas y Cuerpos de Seguridad en tiempo de paz, rebelión y sedición)[41]. En relación con la sedición, cabría plantearse si la reciente aprobación de la Ley Orgánica 14/2022, mediante la que se derogan los preceptos que tipificaban las distintas modalidades de sedición, lleva aparejada la pérdida del carácter extraordinario de los hechos previamente constitutivos de este delito, máxime si tenemos en cuenta que el RSRE, en lugar de prever una definición propia para la sedición, se remite a los tipos penales pertinentes. Esta interpretación, sin embargo, nos llevaría a que la definición contenida en un reglamento (el RSRE) excluyese el carácter extraordinario de unos eventos que el TRECCS (norma con rango de ley) sí enumera como tales. Precisamente por ello, y en la medida en que la mención a la secesión no se suprima del texto del estatuto del CCS, entendemos que los hechos anteriormente constitutivos de tal delito, aunque haya sido destipificado, han de seguir considerándose sucesos catastróficos a efectos de la cobertura del CCS.

La delimitación de los eventos extraordinarios termina de perfilarse, en un sentido negativo, mediante la exclusión de una serie de supuestos. La técnica normativa es semejante: los supuestos excluidos se definen en el RSRE, pero se enumeran en el TRECCS[42]. Algunos de los supuestos excluidos obedecen a la naturaleza asegurativa del CCS (así, se exceptúa la resarcibilidad de los siniestros que no den lugar a indemnización de acuerdo con la LCS); otros se explican por la inexistencia de un auténtico supuesto extraordinario (por ejemplo, el CCS no indemniza los daños producidos por vicio propio de la cosa asegurada); finalmente, existen otros sucesos cuya exclusión solo puede entenderse por cuanto son susceptibles de generar daños tan grandes que trascienden los de un mero suceso catastrófico: así, los daños derivados de la energía nuclear, los que sean calificados por el Gobierno como «catástrofe o calamidad nacional»[43] y los producidos por conflictos armados. Así, la presencia

[41] Las estadísticas del CCS revelan que, en los últimos 25 años, el 95 % de las indemnizaciones se han debido a sucesos de origen natural, frente al 5 % derivado de causas antrópicas. En términos de sucesos concretos, los más significativos son las inundaciones (69 % del total) dentro de los fenómenos naturales, y el terrorismo (4 % del total) dentro de las causas de origen humano (Horrillo Muñoz *et al.*, 2020, p. 2).

[42] Los eventos excluidos por el Estatuto son: los que no den lugar a indemnización de acuerdo con la LCS; los ocasionados en intereses asegurados por contrato de seguro distinto a aquellos en que es obligatorio el recargo; los debidos a vicio o defecto propio de la cosa asegurada; los producidos por conflictos armados, aunque no exista una declaración oficial de guerra; los que por su magnitud y gravedad sean calificados por el Gobierno como «catástrofe o calamidad nacional»; los derivados de la energía nuclear; los debidos a la mera acción del tiempo; o a agentes atmosféricos distintos a los señalados como sucesos catastróficos.

[43] La referencia a la declaración de «catástrofe o calamidad nacional» (que es distinta a la declaración de «zona afectada gravemente por una emergencia de protección civil», comúnmente conocida como «de-

de un elemento bélico excluye la resarcibilidad de los daños producidos tanto por eventos ordinarios (art. 44.1 LSC) como extraordinarios.

Resulta común entre la doctrina, al analizar el sistema de cobertura del CCS, señalar que este opera de forma «cualitativa» (Barrero Rodríguez, 2000, pp. 183 y ss.; García Barona, 1997, p. 406.), es decir, que para delimitar los daños que son resarcibles se tiene en consideración su causa, pero sin exigir que dicha causa se materialice en unos daños especialmente significativos. A la hora de acotar los acontecimientos extraordinarios, la normativa recoge una serie de supuestos que se asume que típicamente son poco frecuentes, y llevan aparejados daños especialmente graves. No obstante, no se tiene en cuenta si efectivamente los supuestos han llevado aparejados daños especialmente graves o no. Los daños consecuencia de un terremoto no necesitan alcanzar un umbral mínimo para ser tildados de catastróficos, sino que llevan aparejada esa condición en la medida en que son consecuencia de un terremoto. La denominación de cualitativo proviene de contrastar el funcionamiento del CCS con otros sistemas de cobertura de riesgos extraordinarios, que exigen que los daños alcancen una determinada entidad para tildar de catástrofe a su causa. Estos últimos serían, pues, denominados como «cuantitativos»[44].

A nuestro entender, sin embargo, lo realmente peculiar del sistema español reside, no en su carácter cualitativo, sino en el momento en que se produce la calificación de un suceso como catastrófico o anormal. Imaginando una sucesión temporal ideal en la que (1) se produce una causa y (2) esa causa lleva a un efecto, algunos sistemas (los que la doctrina denomina «cuantitativos») llevan a cabo la determinación del siniestro como extraordinario en el momento 2, una vez producido el efecto dañoso. El sistema del CCS, no obstante, ya delimita la cobertura del CCS desde el momento de la causa, *ex ante damni*, y con independencia de la entidad del resultado dañoso[45].

---

claración de zona catastrófica» y que en la actualidad se regula mediante la Ley 17/2015, de 9 de julio, del Sistema Nacional de Protección Civil) se regula en el Reglamento sobre seguros agrarios combinados que, a través de su artículo 20, dispone que el Gobierno podrá calificar como tales, siniestros de especial gravedad, teniendo en cuenta su «extensión e importancia». En los casi 70 años de historia del CCS, el Gobierno jamás ha llegado a hacer uso de este instrumento (Consorcio de Compensación de Seguros, 2018, p. 11).

44 Barrero Rodríguez (2000, pp. 183 y ss.) y García Barona (1997, p. 406). Nótese que el primer sistema del CCS, contenido en la Ley de 16 de diciembre de 1954, operaría en términos cuantitativos, ya que, para la cobertura de la mayoría de los acontecimientos catastróficos, resultaba preceptiva una declaración administrativa previa.

45 La única excepción a este funcionamiento *ex ante damni* (y también al carácter cualitativo del CCS) es la declaración como catástrofe o calamidad nacional. No obstante, creemos que su valor reside precisamente en que, por ser una excepción, permite corregir las «deficiencias» del sistema; es decir, un evento que *ex ante* no parece que pueda comportar un riesgo sistémico, para el CCS termina adquiriendo esta entidad *ex post damni*. Así, la declaración permite evitar que el CCS quede expuesto a la cobertura de este riesgo desmesurado.

2.3. Sobre la consideración de los ciberataques patrocinados como actos terroristas

Expuestas las principales características del sistema español de cobertura de los eventos extraordinarios, podemos pasar a discutir si, y bajo qué circunstancias, un ciberataque patrocinado por un Estado puede ser calificado como un suceso catastrófico. Evidentemente, deberemos trabajar con la premisa de que el ciberataque en cuestión ocasiona un daño (por ejemplo, por destrucción o inutilización de los sistemas informáticos, o por la pérdida de beneficio derivada de la parálisis de la actividad) que sea indemnizable de acuerdo con la LCS, sobre un interés ya asegurado por una póliza ordinaria que lleva aparejado el recargo obligatorio a favor del CCS, de acuerdo con el principio de complementariedad adhesiva.

De entre los eventos catastróficos de origen antrópico (terrorismo, motín, tumulto popular, hechos y actuaciones de las Fuerzas Armadas o de las Fuerzas y Cuerpos de Seguridad en tiempo de paz, rebelión y sedición), entendemos que el terrorismo es el único supuesto en el que cabe discutir la subsumibilidad de los ataques patrocinados. Las actuaciones de las Fuerzas Armadas y Fuerzas y Cuerpos de Seguridad se refieren exclusivamente a hechos efectuados por las fuerzas españolas[46]. Por otro lado, resulta artificioso pensar en un ciberataque patrocinado que, por sí mismo, pueda ser calificado como un motín o tumulto popular. Esta conclusión se ve reforzada teniendo en cuenta que el RSRE prevé estas figuras como residuales respecto del terrorismo[47]. Con respecto a los dos últimos fenómenos, la tipificación tanto de la rebelión (art. 544 del Código Penal) como la de la sedición (art. 472, previo a su derogación) requieren la existencia de un alzamiento público (en el sentido de «abierto, exteriorizado, perceptible, patente y manifiesto»)[48] que sea tumultuario y tendente a obstaculizar el normal funcionamiento de las instituciones estatales, en el caso de la sedición; o violento y encaminado a la subversión del orden constitucional, en el de la rebelión. A nuestro parecer, el requisito de una actuación pública es difícilmente conciliable con el *modus operandi* típico del Estado patrocinador de ciberatacantes, que busca actuar de forma insidiosa, aprovechando el anonimato estructural de internet, operando, incluso, a través de un *proxy* para dificultar aún más el proceso de atribución. Por ello, consideramos

46 Ya sean estatales, autonómicas o locales. Véase el artículo 2.1 l) del RSRE.

47 El RSRE define el motín como «todo movimiento acompañado de violencia dirigido contra la autoridad para obtener satisfacción de ciertas reivindicaciones de orden político, económico o social, *siempre que el hecho no tuviese carácter terrorista o fuese considerado tumulto popular*»; y al tumulto como «toda actuación en grupo y con la finalidad de atentar contra la paz pública que produzca una alteración del orden, causando lesiones a las personas o daños a las propiedades, *siempre que el hecho no tuviese carácter terrorista o fuese considerado motín*» (los resaltados son nuestros). La definición de terrorismo, sin embargo, no contempla ninguna salvedad como la que se encuentra al final de las definiciones transcritas («salvo que el hecho tuviese carácter terrorista o fuese considerado motín/tumulto popular»), lo que parece indicar que el terrorismo ejerce una suerte de *vis attractiva* frente a las otras dos figuras, de tal forma que si un mismo hecho es constitutivo de terrorismo, y de motín o tumulto, deberá considerarse como terrorista.

48 STS (Sala de lo Penal) núm. 1049/1980, de 10 de octubre.

difícil pensar en un supuesto de ciberataque patrocinado que pueda revestir dicho elemento de publicidad, esencial tanto para la rebelión como para la sedición.

Centrándonos, pues, en el terrorismo, este se enumera como un fenómeno extraordinario en el artículo 6.1 del TRECCS, y se define en el RSRE como «toda acción violenta efectuada con la finalidad de desestabilizar el sistema político establecido, o causar temor e inseguridad en el medio social en que se produce». El terrorismo constituye un objeto de estudio típico de la disciplina penal, pese a lo cual el RSRE opta por desarrollar este concepto de manera autónoma, en lugar de remitirse a los tipos penales pertinentes. La definición contenida en el reglamento se integra por dos elementos: uno que podríamos tildar de objetivo (que se lleve a cabo una actividad violenta) y otro subjetivo-teleológico (que se persiga la finalidad de «desestabilizar el sistema político establecido, o causar temor e inseguridad en el medio social en que se produce»). De esta manera, el RSRE no condiciona la existencia del terrorismo a las características del sujeto terrorista. Al contrario, la persecución de las finalidades mencionadas basta para hacer de una acción violenta un suceso catastrófico a efectos de su cobertura por el CCS[49].

El elemento objetivo de la definición requiere que la actuación terrorista sea una acción (con lo que parece descartarse la posibilidad de un «terrorismo omisivo»), y que sea violenta. La violencia, entendemos, está asociada al uso de una fuerza susceptible de provocar un resultado dañoso[50]. Esta caracterización de lo violento como aquello que es idóneo para generar daños en el contexto del derecho de seguros ya la propone Sánchez Calero (2010, p. 2.611) en el comentario de la definición de accidente contenida en el artículo 100 de la LCS.

La segunda parte de la definición se refiere a la persecución de una finalidad terrorista concreta. A nuestro juicio, este elemento subjetivo no puede interpretarse como completamente aislado del tipo de acción violenta escogida. Lo que diferencia a los acontecimientos catastróficos, como hemos visto, es principalmente su imprevisibilidad y su capacidad de causar grandes daños. Por ello, creemos que el hecho de que una acción violenta se efectúe, en el fuero interno de su autor, con una finalidad terrorista no basta para categorizarla como tal. Así, entendemos que la finalidad última debe tener un cierto reflejo en el tipo de

[49] A pesar de la autonomía de la acepción de terrorismo empleada por el RSRE respecto a la penal, existen similitudes evidentes entre ambas, particularmente a raíz de la reforma llevada a cabo por la Ley Orgánica 2/2015. Nuestra doctrina penalista (por todos, Pastrana Sánchez [2020, p. 51]) afirmaba que clásicamente el terrorismo (que en el Código Penal de 1995 no se abordaba como un único delito, sino como una modalidad de otras figuras delictivas) se caracterizaba por la presencia de dos elementos: por un lado, la existencia de una organización, una estructura relativamente duradera, estable y jerárquica (el denominado elemento estructural; a pesar de que, de forma marginal, se contemplasen modalidades de terrorismo individual [Mosquera Blanco, 2022, pp. 10-11]), y la persecución de unos fines de índole política (el elemento finalista o teleológico). Sin embargo, a raíz de la aprobación de la Ley Orgánica 2/2015, el requisito del elemento estructural desaparece casi por completo (Pastrana Sánchez, 2020, p. 205), con lo que la calificación de la actividad terrorista como tal pasa a depender de que a través de la misma se persiga alguno de los fines de índole política referidos en el artículo 573 del CP.

[50] *Violentus* deriva directamente de *vis* (fuerza).

acción violenta por la que se ha optado, en el sentido de que esta debe ser, al menos, mínimamente idónea como para poner de manifiesto el objeto perseguido. Por ejemplo, un ciberataque de tipo *ransomware*, mediante el que se exige un rescate a una empresa de tamaño mediano, sin que el incidente se revele ni se reivindique públicamente, aunque se efectúe con la finalidad de desestabilizar el sistema político, tendrá menos posibilidades de ser considerado terrorista que un ataque que paraliza el funcionamiento de una infraestructura esencial y se reivindica públicamente por un grupo posicionado políticamente. A nuestro parecer, el elemento subjetivo debe tener una influencia, siquiera tangencial, en el elemento objetivo; dicho de otra forma, el fin último debe verse reflejado en los medios empleados.

Visto lo anterior, podemos pasar a discutir si un ciberataque patrocinado por un Estado puede considerarse un acto terrorista a efectos del RSRE. Nuestra respuesta es, en principio, afirmativa. Para comenzar, un ciberataque puede ser considerado, sin mayor problema, una «acción violenta». Como hemos justificado, la violencia debe entenderse como idoneidad para provocar daños. A este respecto, la doctrina moderna reconoce la posibilidad de expresiones violentas no corpóreas[51]. En la medida en que un ciberataque puede provocar resultados dañosos sobre activos digitales o físicos (por ejemplo, inutilizando o destruyendo un equipo informático), creemos que puede ser considerado como una acción violenta.

En cuanto al elemento subjetivo-teleológico, también entendemos que podría concurrir sin mayores problemas. Según apuntamos en la introducción, una gran parte de los ciberataques patrocinados tienen efectos puramente destructivos, y se emplean de forma instrumental para minar la estabilidad social y la confianza en los líderes políticos, siendo el NotPetya un ejemplo paradigmático: un *malware* dirigido contra equipos ucranianos que acaba provocando una auténtica crisis política e institucional[52].

La conclusión anterior no se ve afectada por el hecho de que el ciberataque sea atribuible a un Estado. En la medida en que la definición del RSRE no contiene exigencia alguna con respecto al sujeto activo, pudiendo este ser, en teoría, un solo individuo, o un grupo organizado, no creemos que el hecho de que la acción terrorista sea llevada a cabo por un Estado impida categorizar un ciberataque como terrorista.

En suma, la consideración de un ciberataque como evento extraordinario a efectos de su cobertura por el CCS dependerá en la gran mayoría de casos de su consideración como

---

[51] Véase la interpretación del concepto que hace la Sala Segunda del Tribunal Supremo en la Sentencia núm. 615/2019, de 11 de diciembre, FJ 3.º. A pesar de pertenecer al orden penal, dicha resolución es pertinente, ya que interpreta el concepto de violencia contenido en el Diccionario de la RAE. Por otro lado, Sánchez Calero (2010) menciona como sucesos que pueden ser violentos (en cuanto potencialmente dañosos) la asfixia por gases o agua, o el envenenamiento.

[52] La entidad de la desestabilización a la que es capaz de dar lugar un ciberataque patrocinado se hace patente en las declaraciones del ministro de infraestructura ucraniano Volodymyr Omelya, que, en el contexto de los efectos del NotPetya, llegó a afirmar que «fue un bombardeo masivo sobre todos nuestros sistemas […] el gobierno estaba muerto» (Greenberg, 2018).

acto terrorista, según se desarrolla en el RSRE. Decíamos que, en la práctica totalidad de situaciones, un ciberataque causante de un daño conllevará la comisión de un ilícito civil o penal, con lo que será constitutivo de acciones violentas (elemento objetivo de la definición). La cuestión sobre el carácter (extra)ordinario del ataque pasa entonces a pivotar sobre el elemento subjetivo, esto es, sobre la concurrencia de una «finalidad de desestabilizar el sistema político establecido, o causar temor e inseguridad en el medio social». Justificábamos antes que la finalidad con la que obra el cibercriminal no debe ser relevante a efectos de la trascendencia aseguradora del ataque, a menos que dicha finalidad tenga un reflejo mínimo en el tipo de acción violenta escogida.

La trascendencia que otorga la ley al elemento subjetivo de la acción terrorista colisiona con la realidad de la cibercriminalidad, en la que, según advertíamos en la introducción, las líneas que separan las acciones de los Estados y de los grupos independientes son tan etéreas como las que delimitan las finalidades económicas y políticas. Esta cuestión es paradigmática en los ataques de tipo *ransomware*, en los que se bloquean los equipos informáticos del sujeto afectado, exigiendo un rescate por la liberación de los mismos. Si bien su funcionamiento parecería evidenciar un ánimo económico y, por ende, no político, los antecedentes nos muestran múltiples casos de *ransomware* dirigidos contra infraestructuras críticas o directamente gubernamentales, que han provocado situaciones de gran inestabilidad política y social en los Estados afectados, y en los que resulta más que razonable sospechar que el ánimo de lucro es secundario, o directamente una tapadera[53].

Sería iluso, pues, tratar de establecer un único criterio que permitiese diferenciar los ataques motivados política y económicamente. Al contrario, lo que aquí proponemos es que dicha evaluación debe realizarse *in casu*, atendiendo a todas las circunstancias relacionadas con cada ataque en cuestión y el contexto en que se produce. Algunos de los elementos a considerar podrían ser, *inter alia*, la idoneidad del ataque para generar inestabilidad política o temor social, o para beneficiar económicamente al atacante; la situación geopolítica en que se produce; si el ataque se ha atribuido a algún grupo concreto (y, en caso afirmativo, los antecedentes del mismo); o el tipo de entidad(es) afectada(s).

Como paradigma de un ataque motivado políticamente podríamos pensar en el NotPetya, con efectos netamente destructivos sobre los equipos afectados y susceptible de perturbar la situación política y social de todo un Estado, produciéndose, además en un contexto diplomático hostil entre el Estado patrocinador (Rusia) y el Estado afectado (Ucrania). Al contrario, un ejemplo ideal de ciberataque con una motivación económica sería uno en el que se accede a los sistemas informáticos de una entidad de dimensión reducida para llevar a cabo una disposición patrimonial a favor de los atacantes, sin mayores repercusiones. Entre estos dos extremos existe un continuo de situaciones posibles que revisten con mayor o menor intensidad las características de un ciberataque terrorista. Aquellos casos

[53] De nuevo nos referimos al caso del grupo criminal Conti y a las injerencias del gobierno ruso en su proceso de selección de objetivos.

«grises» en los que no pueda deducirse de forma suficientemente clara la persecución de una finalidad terrorista deberían ser considerados, a nuestro parecer, como eventos ordinarios. La excepcional intervención del CCS se determina *ex ante damni*, atendiendo a la causa de los daños y con independencia de la frecuencia de los eventos y la cuantía de los perjuicios. Por ello, una interpretación laxa de los supuestos extraordinarios podría implicar que el consorcio desplazase a las aseguradoras privadas en supuestos que distan demasiado de aquellos que fundamentaron su creación.

Que el ataque se lleve a cabo por un Estado o no resulta irrelevante para la determinación de su naturaleza extraordinaria, en la medida en que la definición de terrorismo no depende de la identidad del sujeto terrorista. Dado el elemento objetivo de la acción violenta, será el elemento subjetivo-teleológico el que determine si el evento es extraordinario (recayendo, en caso de que concurran los demás requisitos –previo pago del recargo, transcurso del periodo de carencia, etc.– en el ámbito del CCS) u ordinario (correspondiendo su cobertura a la póliza privada). Sin embargo, podría discutirse si la identidad del atacante podría tener relevancia, en caso de que determine la consideración del ataque como derivado de un conflicto armado.

3. Ciberataques patrocinados como eventos excluidos

3.1. De la guerra al conflicto armado

En el apartado anterior hemos tratado de discernir las circunstancias que determinan que la cobertura de un ciberataque sea asumida por la aseguradora privada o por el CCS. No obstante, nuestro análisis no se detiene ahí. Los daños producidos por conflictos armados vienen excluidos de la cobertura tanto de las pólizas privadas (art. 44 LCS, salvo pacto en contrario) como del consorcio (art. 6.3.d TRECCS). Determinado el carácter (extra)ordinario de un ciberataque patrocinado, todavía debemos responder a la cuestión sobre si se puede considerar que el mismo ha sido producido por un conflicto armado, lo que eximirá de responsabilidad a la aseguradora privada o al consorcio, según sea el caso.

A lo largo de las páginas siguientes nos referiremos a las exclusiones de los daños derivados de conflictos armados contenidas en la LCS y en el TRECCS como *exceptio belli*. Antes apuntábamos que la exclusión bélica es tradicional en nuestro derecho, y también lo es la ausencia de una definición concisa de los fenómenos cubiertos por dicha exclusión[54]. En este sentido, e incluso excediendo el campo del derecho de los seguros, no existen en nuestro ordenamiento interno pautas para diferenciar de forma clara qué se entiende por

[54] El Decreto de 13 de abril de 1956 sí incluía una suerte de definición sobre el fenómeno del conflicto armado, en su artículo 9 b): «entendiendo por tal la guerra civil o internacional, haya o no mediado declaración oficial». Como se podrá constatar, más allá de la mención a la posibilidad de que se dé un conflicto armado, aún sin mediar una declaración oficial, el valor interpretativo de la definición es escaso.

conflicto armado[55]. Esta ausencia se explica en parte por la dificultad que comporta delimitar conceptualmente el fenómeno bélico. Así, la experiencia empírica demuestra que la calificación de un suceso violento como conflicto armado depende en múltiples ocasiones de factores culturales, así como de intereses estratégicos y geopolíticos por parte de los distintos integrantes de la comunidad internacional (Geneva Association, 2020, p. 12).

Lo primero que debemos señalar es que el concepto empleado por el TRECCS, así como por la LCS en su redacción actual, es el de «conflicto armado». Esto contrasta con la dicción de la LCS anterior a 1990, que excluía los daños «por hechos de guerra civil o internacional»[56]. La opción del legislador español, lejos de ser casual, refleja una tendencia del derecho internacional público hacia la utilización del término de conflicto armado en detrimento del de guerra, típicamente asociado a la existencia de una declaración formal por parte de los combatientes y que, hasta la primera mitad del siglo XX, era considerada la forma paradigmática de violencia interestatal. El desuso del concepto de guerra coincide, para la mayoría de los autores, con la aprobación de la Carta de las Naciones Unidas en 1945, y la prohibición del uso de la fuerza que, como regla general, establece el artículo 2(4) de dicho texto (O'Connell y Gardam, 2010, p. 7). La Carta de las Naciones Unidas no logró erradicar las hostilidades entre Estados, pero existe evidencia empírica de que, a raíz de su aprobación, las declaraciones formales de guerra se volvieron cada vez menos frecuentes (O'Connell y Gardam, 2010).

Esa evolución comportaba un desafío para la aplicación de una serie de normas que se supeditaban a la existencia de una declaración de guerra, tales como las de derecho internacional humanitario contenidas en las Convenciones de La Haya de 1899 y 1907, o en los convenios de Ginebra de 1864, 1906 y 1929[57]. La solución pasó por acuñar un término que describiese la existencia de fenómenos de naturaleza bélica, pero cuya existencia no dependiese de una previa declaración formal de guerra: el conflicto armado.

Resulta común referirse al primero de los cuatro convenios de Ginebra[58], de 1949, como el primer instrumento de derecho internacional público en hacer uso del concepto de conflicto armado. Estos convenios, junto con sus protocolos adicionales, constituyen las principales fuentes de derecho internacional humanitario, y persiguen dos objetivos principales:

---

55 Otras normas de nuestro ordenamiento que dan relevancia jurídica a fenómenos bélicos sin llegar a definirlos son la Ley 12/2009, de 30 de octubre, reguladora del derecho de asilo y de la protección subsidiaria, o el Real Decreto-ley 14/2001, de 28 de septiembre, por el que se establece el régimen del reaseguro por cuenta del Estado de los riesgos de guerra y terrorismo que puedan afectar a la navegación aérea.

56 Si bien la normativa reguladora del CCS (Ley de 16 de diciembre de 1954 y su reglamento de desarrollo) ya utilizaban el término de conflicto armado.

57 Los instrumentos citados incluían una serie de normas de *ius in bello*, pero sin determinar bajo qué criterios devenían aplicables. No obstante, se entendía que su aplicabilidad dependía de la existencia de una declaración oficial de guerra (Henckaerts y Comité Internacional de la Cruz Roja, 2016, par. 192).

58 I Convenio de Ginebra para aliviar la suerte que corren los heridos y los enfermos de las fuerzas armadas en campaña, 1949. https://www.icrc.org/es/doc/resources/documents/treaty/treaty-gc-1-5tdkna.htm

la prohibición del uso de determinados métodos o medios de hacer la guerra y la protección de los individuos que, a pesar de verse envueltos en un conflicto armado, no participan en las hostilidades (Kaczorowska, 2015, p. 762). Los convenios de Ginebra han sido ratificados por 196 Estados (esto es, son de aplicación prácticamente universal)[59].

El Primer Convenio de Ginebra distingue entre dos grandes clases de conflictos armados, según estos sean internacionales (art. 2 del convenio) o no (art. 3). Esta diferenciación es muy relevante, ya que las normas de derecho internacional humanitario aplicables varían según nos encontremos ante un tipo de conflicto u otro[60].

El artículo 3 del primer convenio establece una serie de disposiciones que resultan aplicables a los conflictos armados que enfrentan a un Estado con un grupo no estatal, o incluso a varios grupos no estatales entre sí. No cualquier expresión violenta dentro del territorio de un Estado basta para dar inicio a un conflicto armado intraestatal. En este sentido, una interpretación extensiva de este concepto llevaría a una aplicación sistemática del derecho internacional humanitario a hechos puramente internos. Así, las situaciones de meras «tensiones internas y de disturbios interiores, tales como los motines, los actos esporádicos y aislados de violencia y otros actos análogos»[61] no constituyen conflictos armados a efectos de la aplicación artículo 3, con lo que quedan sujetos al derecho interno de cada Estado. Para diferenciar los conflictos armados no internacionales de estas otras formas menos graves de violencia, el criterio mayoritario señala que las hostilidades deben alcanzar una cierta intensidad, así como involucrar a actores dotados de un determinado grado de organización (Comité Internacional de la Cruz Roja, 2008, pp. 3-4).

La intensidad se refiere al grado de violencia que deben alcanzar las disputas. Conforme a la jurisprudencia, esta se determina de acuerdo con factores como la dispersión temporal y geográfica de los enfrentamientos, el tipo de armamento empleado, o el número de civiles desplazados, entre otros[62]. El requisito de la organización, a su vez, alude a la estructura

---

59 Lista completa en https://ihl-databases.icrc.org/en/ihl-treaties/gci-1949/state-parties. Adicionalmente, un gran número de las provisiones contenidas en los Convenios de Ginebra han venido siendo consideradas como normas de derecho internacional consuetudinario, por lo que su obligatoriedad no depende de su ratificación por parte de un Estado (Kaczorowska, 2015, p. 762).

60 Así, las provisiones establecidas para los conflictos internacionales son mucho más extensas y detalladas que para los conflictos no internacionales, hasta el punto de que el artículo 3 del primer convenio (que contiene las normas aplicables a estos últimos, sin perjuicio de las normas especiales contenidas en el Protocolo Adicional II) se ha llegado a denominar de forma coloquial como un «convenio en miniatura» (Henckaerts y Comité Internacional de la Cruz Roja, 2016, par. 356). Esta diferencia se debe a la reticencia de los Estados a que el derecho internacional humanitario regule con demasiado detalle situaciones puramente internas.

61 Artículo 1 del Protocolo II adicional a los Convenios de Ginebra de 1949. A pesar de que esta exclusión no está contenida dentro del texto del artículo 3 del Primer Convenio de Ginebra, la opinión mayoritaria es que también le resulta aplicable (Henckaerts y Comité Internacional de la Cruz Roja, 2016, par. 386).

62 *Prosecutor v. Boskoski and Tarculovski* (Trial Judgment), IT-04-82-T, Tribunal Penal Internacional para la Antigua Yugoslavia (TPIY), 10 de julio de 2008. https://www.refworld.org/cases,ICTY,48ac30e22.html, par. 177.

de las partes, y a su capacidad para llevar a cabo actividades militares de forma sostenida en el tiempo, atendiendo, entre otros elementos, a la existencia de una estructura jerárquica, o a la capacidad de coaccionar a los miembros del grupo en caso de desobediencia[63].

En contraposición con los conflictos internos, los conflictos armados internacionales son los que enfrentan a dos o más Estados. Desde la perspectiva del derecho internacional humanitario, la existencia de un conflicto armado internacional se ha venido determinando mediante unos criterios relativamente amplios. Así, el Comité Internacional de la Cruz Roja (CICR, principal promotor de las convenciones de Ginebra, y al que las mismas asignan expresamente múltiples funciones en su condición de guardián del derecho internacional humanitario)[64], al igual que varios autores, entiende que cualquier forma de confrontación armada entre Estados constituye un conflicto armado, sin que exista un requisito mínimo de violencia o intensidad en las hostilidades[65]. Este criterio parece ser consecuente con la definición generalmente aceptada de conflicto armado internacional, que fue la que utilizó el Tribunal Internacional Penal para la Antigua Yugoslavia en el caso Tadic, determinando que «un conflicto armado existe siempre que hay un recurso a la violencia armada entre Estados»[66]. La existencia del conflicto no depende de que concurra una declaración de guerra, ni siquiera de que sea reconocido por los combatientes, sino de las circunstancias fácticas realmente existentes[67]. La violencia puede proyectarse sobre las instalaciones militares del Estado atacado, pero también sobre su infraestructura civil o población en general.

De acuerdo con el criterio del CICR, cualquier forma de violencia da lugar a la aplicabilidad del convenio, aunque se trate de meras escaramuzas o enfrentamientos puntuales entre las fuerzas armadas de dos Estados (David, 2008, p. 109). No es necesario que la violencia se

63 *Ibidem*, par. 195-197.

64 Una mención a estas funciones se puede encontrar en Mazzuoli (2017, pp. 374 y ss.).

65 En un documento de opinión de 2008, el CICR sostenía que «un [conflicto armado internacional] ocurre cuando uno o más Estados recurren a la fuerza armada contra otro Estado, sin tener en cuenta las razones o la intensidad del enfrentamiento. Las normas pertinentes del [derecho internacional humanitario] pueden ser aplicables incluso si no hay hostilidades abiertas» (2008, p. 1).

66 *Prosecutor v. Dusko Tadic alias «Dule»* (Decisión sobre la petición de la defensa de apelación interlocutoria sobre la jurisdicción), IT-94-1, Tribunal Penal Internacional para la Antigua Yugoslavia (TPIY), 2 de octubre de 1995. https://www.refworld.org/cases,ICTY,47fdfb520.html, párr. 70. Sin embargo, dentro del mismo párrafo, el tribunal parece insinuar que sí existe un requisito de intensidad en las hostilidades para declarar la existencia de un conflicto armado internacional. Así, al referirse a los enfrentamientos que tuvieron lugar en la antigua Yugoslavia, se dice que «estas hostilidades excedieron los *requisitos de intensidad aplicables tanto a los conflictos armados internacionales* como a los internos» (destacados y traducción nuestros).

67 Esto no quiere decir que la existencia de una declaración sea totalmente irrelevante a efectos de la aplicación del Convenio de Ginebra, ya que una declaración formal de guerra basta para provocar la aplicabilidad del convenio, aunque no vaya seguida de violencia armada (Henckaerts y Comité Internacional de la Cruz Roja, 2016, par. 206). En otras palabras, el convenio es aplicable tanto si existe violencia armada entre Estados como si un Estado declara la guerra.

materialice a través de ningún medio o método de guerra específico. Esto es muy relevante para nuestro análisis ya que, de acuerdo con el CICR, un ciberataque imputable a un Estado podría bastar para entender iniciado un conflicto armado siempre que provoque daños en otro Estado análogos a los que se podrían ocasionar a través de medios o métodos de guerra tradicionales. Según el Comentario de 2016 al artículo 2 del Primer Convenio de Ginebra, elaborado por el CICR,

> las ciberoperaciones con efectos similares a las operaciones cinéticas clásicas pueden constituir un conflicto armado internacional. De hecho, si estas operaciones provocan la destrucción de activos civiles o militares, o causan la muerte o lesiones a soldados o civiles, no habría razón para tratar la situación de forma diferente a los ataques equivalentes realizados con medios y métodos de guerra más tradicionales[68].

¿Quiere esto decir que, en todo caso, cualquier expresión de violencia armada dirigida de un Estado a otro basta para entender iniciado un conflicto armado? No tiene por qué. El criterio del CICR es enormemente ilustrativo, en la medida en que no deja de ser el organismo promotor del principal cuerpo de normas de *ius in bello*, y pionero en hacer un uso sistemático del concepto de conflicto armado. No obstante, existe evidencia empírica robusta que vendría a señalar que, en la práctica, no toda forma de violencia interestatal recibe el calificativo de conflicto armado internacional.

En 2010, la International Law Association hizo público uno de los trabajos de sistematización más exhaustivos en lo que al concepto de conflicto armado se refiere (O'Connell y Gardam (2010). Motivado por las dudas sobre el empleo del término «guerra al terror» (*war on terror*) por parte de Estados Unidos, el informe recopila múltiples tratados, decisiones judiciales y de otros organismos internacionales, además de opiniones doctrinales, para tratar de discernir la esencia común que subyace a los distintos conflictos armados, concluyendo que, en la práctica, la noción de conflicto armado no se emplea para designar toda forma de hostilidad intraestatal ni interestatal. Al contrario, los conflictos armados internacionales también están sometidos a unos requisitos de organización e intensidad mínima (pp. 32-33). Prácticamente todo Estado, por el hecho de tener tal condición, estará dotado de la organización necesaria para llevar a cabo violencia armada de forma sostenida (p. 29); precisamente por ello, es la intensidad de la violencia (concretada en factores como el número de soldados involucrados, el tipo de armas empleadas, los daños personales y materiales ocasionados, la extensión geográfica y temporal, etc.) (p. 30) la que diferencia a los conflictos armados de otras formas de violencia entre Estados de naturaleza menos severa.

Posiblemente, el argumento más contundente a favor de la tesis defendida por el informe es el gran número de intercambios de violencia armada entre Estados acontecidos tras

[68] Traducción propia (Henckaerts y Comité Internacional de la Cruz Roja, 2016, par. 255). A esta misma conclusión llegaron los expertos que elaboraron el *Manual de Tallín sobre el derecho internacional aplicable a la ciberguerra* (véase la regla 20).

1945 y que no recibieron el tratamiento propio de un conflicto armado, por no alcanzar un umbral de violencia mínimo, recibiendo calificativos como el de «enfrentamientos fronterizos» o «incidentes navales» (O'Connell y Gardam, 2010, pp. 13-14, 18 y 26-27)[69].

¿A qué se debe esta diferencia entre el criterio del CICR y los hallazgos de la International Law Association? El objetivo de las normas de derecho internacional humanitario (y, consecuentemente, el del CICR) no es otro que el de maximizar la protección de los sujetos que se ven envueltos en situaciones de hostilidad, lo que justifica el uso de una acepción amplia de conflicto armado interestatal, que no requiere un nivel mínimo de violencia. Al fin y al cabo, establecer un umbral de violencia que condicione la aplicabilidad de las normas de derecho internacional humanitario implicaría diferenciar de manera injustificada entre las víctimas de unos conflictos y de otros (o, incluso, dentro de un mismo conflicto, entre las víctimas que se ven afectadas antes y después de que el nivel de violencia alcance el propio del conflicto armado)[70]. La persecución de dicho objetivo justifica, pues, que el CICR emplee una noción de conflicto armado que comprenda toda forma de violencia armada interestatal.

En cualquier caso, para que una situación de hostilidad dé lugar a un conflicto armado internacional es necesario que involucre, al menos, a dos Estados, por lo que resulta necesario poder imputar las actuaciones violentas a los Estados participantes. Para tal atribución, las normas de derecho internacional no exigen que las actividades sean obra de sus fuerzas militares, bastando que se efectúen por parte de cualquier sujeto o entidad a la que se reconozca un estatus en el derecho interno del Estado atacante o que, de cualquier otra manera, venga facultado jurídicamente para ejercitar alguna forma de poder público[71]. Adicionalmente, también se puede imputar a un Estado la actuación de un grupo que no ejercita poder público *de iure*, siempre que este actúe bajo su control fáctico[72]. El grado de control que el Estado debe ostentar sobre su agente *de facto*, no obstante, no es una cuestión pacífica doctrinal ni jurisprudencialmente. Existe un debate entre aquellos que requieren que el control sea «efectivo» y los que estimarían que un mero «control global»

---

69 El tratamiento como conflicto armado (o su ausencia) se deducen de resoluciones judiciales, resoluciones del Consejo de Seguridad de las Naciones Unidas, de comentarios doctrinales, o de la respuesta de los propios Estados afectados, entre otras fuentes.

70 Este argumento se puede resumir con el siguiente extracto del Comentario de 1952 al artículo 2 del Primer Convenio de Ginebra, elaborado por Jean Pictet: «Resulta irrelevante cuánto dure el conflicto, o cuántas matanzas tengan lugar. El respeto por la personalidad humana no se mide a través del número de víctimas» (traducción propia) (par. 1).

71 Véanse los artículos 4.2 y 5 del Proyecto de artículos sobre la responsabilidad del estado por hechos internacionalmente ilícitos. https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf. Las convenciones de Ginebra no incluyen reglas relativas a la imputabilidad de los Estados, es por ello que debemos acudir al Proyecto de Artículos, elaborado por la Comisión de Derecho Internacional de las Naciones Unidas, y considerada la principal compilación de derecho consuetudinario en lo relativo a atribución de responsabilidad a los Estados.

72 Artículo 8 del Proyecto de artículos sobre la responsabilidad del estado por hechos internacionalmente ilícitos.

basta para atribuir al Estado las acciones del agente. El control global se alcanzaría cuando el Estado ofrece financiación y equipamiento al grupo, además de asistir en la planificación general de sus actividades, mientras que el control efectivo, además de lo anterior, requiere que el Estado supervise o intervenga en todas y cada una de las operaciones del grupo para que estas le sean imputadas. Entre los que han abogado por el criterio del control global se encuentran el Tribunal Internacional Penal para la Antigua Yugoslavia o la Corte Penal Internacional[73]. La Corte Internacional de Justicia, por su parte, se ha posicionado como el principal defensor del criterio del control efectivo para determinar la responsabilidad de un Estado[74]. Sin embargo, a efectos exclusivamente de discernir si una situación puede ser considerada un conflicto armado o no (sin que ello determine la responsabilidad estatal), la propia Corte Internacional de Justicia ha reconocido que el test del control global puede ser adecuado[75].

Este punto es vital en la discusión sobre la atribución de ciberataques, dada la tendencia de los Estados a llevar a cabo estas actividades mediante *proxies*. Usando el criterio del control global, bastaría con que un Estado financie y equipe a un grupo, además de orientarle de forma general sobre el tipo de actividades que debe llevar a cabo, para que se le considere un agente estatal *de facto*. Sin embargo, el estándar del control efectivo es más estricto, ya que requiere que el Estado participe en la preparación de cada uno de los ataques llevados a cabo por el grupo para que estos se le pudiesen atribuir.

3.2. Sobre la consideración de los ciberataques patrocinados como constitutivos de conflictos armados

Una vez estudiado el origen y la aplicación del concepto de conflicto armado, podemos pasar a dar respuesta a la pregunta sobre si, y en qué condiciones, la *exceptio belli* puede resultar de aplicación a un ciberataque patrocinado por un Estado. En este sentido, queremos adelantar que, desde nuestra perspectiva, consideramos altamente improbable que un ciberataque patrocinado por un Estado –según las características que estos revisten en la actualidad– quede excluido por considerarse como derivado de un conflicto armado.

---

73 *Prosecutor v. Dusko Tadic* (Appeal Judgement), IT-94-1-A, Tribunal Penal Internacional para la Antigua Yugoslavia (TPIY), 15 de julio de 1999. https://www.refworld.org/cases,ICTY,40277f504.html, par. 131; *Prosecutor v. Lubanga (Decision on Confirmation of Charges), ICC-01/04-01/06*, Corte Penal Internacional (CPI), 29 de enero de 2007, par. 211.

74 *Case Concerning Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. United States of America)*; Merits, Corte Internacional de Justicia (CIJ), 27 de junio de 1986. https://www.refworld.org/cases,ICJ,4023a44d2.html, par. 115; *Case Concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia-Herzegovina v. Yugoslavia)*, Corte Internacional de Justicia (CIJ), 11 de julio de 1996. https://www.refworld.org/cases,ICJ,4040ba0c4.html, par. 392–393

75 *Case Concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia-Herzegovina v. Yugoslavia)*, par. 404.

A la luz del apartado anterior, consideramos que las exclusiones derivadas de la existencia de conflictos armados contenidas en la LCS y en el TRECCS solo deben aplicarse en casos de conflictos armados, internacionales o no, que reúnan los requisitos de intensidad de las hostilidades y organización de las partes (para lo cual será necesario imputar el conflicto a un sujeto agente).

Evidentemente, tal postura implica apartarnos del criterio del CICR. Reconocer la importancia que en el campo del derecho internacional humanitario tiene el comité no implica asumir sus posturas de manera acrítica. Las conclusiones del comité persiguen un objetivo: el de maximizar la protección que ofrecen las normas de *ius in bello*; finalidad ajena a las normas que disciplinan el derecho de seguros, en las que de la calificación de una situación como conflicto armado no se desprenden consecuencias a nivel humanitario. Acoger sin matices el criterio del CICR implicaría afirmar que cualquier ciberataque llevado a cabo por un Estado extranjero que provoca daños en España supone el inicio de un conflicto armado.

El artículo 3.1 de nuestro Código Civil nos obliga, a la hora de interpretar una norma jurídica, a acudir en primer lugar a su sentido literal, es decir, a examinar los fenómenos a los que comúnmente se alude empleando el concepto controvertido. El enfoque del informe de la International Law Association opera de forma positiva en lugar de normativa; dicho de otra manera, se centra en averiguar lo que un conflicto armado es (a través de las situaciones que comúnmente se califican como tal) en lugar de lo que debería ser. Si, de acuerdo con sus conclusiones, los distintos conflictos armados presentan ciertos elementos de intensidad y organización, creemos que es precisamente la concurrencia de dichos elementos la que debe ser considerada para valorar si estamos o no ante un conflicto armado.

Esta conclusión se apoya en otros argumentos. En lo que atañe a la cobertura del CCS, el texto del TRECCS, a la hora de enumerar los acontecimientos extraordinarios que sí dan lugar a indemnización se refiere, en su artículo 6.1 c), a los «hechos o actuaciones de las Fuerzas Armadas o de las Fuerzas y Cuerpos de Seguridad en tiempo de paz». Este último matiz («en tiempo de paz») parece una referencia a la exclusión por conflictos armados, en el sentido de que los daños producidos por las Fuerzas Armadas, o por las Fuerzas y Cuerpos de Seguridad, dejan de ser indemnizables en caso de concurrir *exceptio belli*. De lo anterior se deduce una nueva característica (negativa) de la noción de conflicto armado manejada por el legislador: una situación de tiempo de no-paz. El conflicto armado revela así una cierta dimensión temporal, una suerte de aptitud para interrumpir un tiempo de paz e iniciar un tiempo de conflicto. Un ataque esporádico no parece ajustarse a esta noción de conflicto armado.

Parece, pues, que los que defiendan una interpretación que considere todo supuesto de violencia interestatal como conflicto armado deberán abogar por una interpretación extensiva de dicho concepto jurídico indeterminado. Dicho de otra manera, se estaría proponiendo incluir en una norma de naturaleza restrictiva para los derechos del asegurado supuestos que no parecen cubiertos por la literalidad del precepto. Esto atenta contra principios ver-

tebradores de nuestro ordenamiento como son el de la reparación íntegra del daño, y más concretamente el de *in dubio pro damnato*[76].

3.2.1. Requisito intensivo

No existe consenso acerca del nivel concreto de intensidad que distingue al conflicto armado de otras formas de enfrentamientos violentos. En el derecho internacional público, los distintos tribunales y autores coinciden en que la apreciación debe efectuarse *in casu*, atendiendo a todas las circunstancias relevantes que envuelven a las hostilidades. No obstante, no creemos que un ciberataque (o una campaña de ciberataques) patrocinado por un Estado pueda, por sí mismo, alcanzar dicho umbral, al menos basándonos en aquellos ataques de los que tenemos constancia en el momento presente.

No cabe duda de que en los últimos años han existido ciberataques con consecuencias muy severas. Más allá del NotPetya, en 2010, el *malware* Stuxnet provocó daños físicos en centrifugadoras nucleares de Irán, que se estima que retrasaron hasta dos años su programa nuclear (Sanger, 2012). En 2017, un *ransomware* paralizó durante una semana las actividades de Colonial Pipeline, que gestiona la mayor red de oleoductos de petróleo refinado en Estados Unidos, provocando escasez y subidas de precio generalizadas (Bing y Kelly, 2021). Los efectos de estos ataques (y de muchos otros) no son para nada desdeñables, pero no parecen aproximarse a la entidad de las consecuencias de un conflicto armado.

Para tener una idea aproximada del grado de violencia propio de un conflicto armado, el informe de la International Law Comission se refiere (O'Connell y Gardam, 2010, p. 23) a los enfrentamientos entre integrantes del Movimiento Todos por la Patria y las fuerzas del ejército argentino, que tuvieron lugar en el cuartel de La Tablada en 1989, como el conflicto armado de menor intensidad en ser calificado como tal por un organismo internacional o tribunal[77]. A pesar de que las hostilidades no se prolongaron más de 30 horas, requirieron la intervención directa de personal militar, y provocaron la muerte de más de 29 personas, además de múltiples heridos y daños materiales significativos[78].

Lo anterior no debe ser tomado como un límite absoluto, en el sentido de que las hostilidades que involucren un grado de violencia menor que los acontecimientos de La Tablada

---

[76] En tanto el concepto de conflicto armado tiene su origen en disposiciones legales (arts. 44 de la LCS y 6.3.d del TRECCS), y no contractuales, debe atenderse al principio de *in dubio pro damnato* y no el de *in dubio pro asegurado*, que dimana de los artículos 3 de la LCS y 1.288 del Código Civil y exige una interpretación favorable de las disposiciones contractuales (véase la STS 347/2009, de 18 de mayo, FJ 7.º). Otra cosa será la interpretación de las cláusulas limitativas de las pólizas privadas que excluyan eventos bélicos y similares más allá del tenor del artículo 44 de la LCS, como discutiremos más adelante.

[77] En este caso, por la Comisión Interamericana de Derechos Humanos, en el caso *Juan Carlos Abella v. Argentina*, caso 11.137, informe 55/97. https://www.cidh.oas.org/annualrep/97span/Argentina11.137.htm#_ftn2

[78] *Juan Carlos Abella v. Argentina*, par 1, 152-156.

no puedan ser calificadas como conflictos armados, pero permite ilustrar la diferencia entre la intensidad que típicamente caracteriza a las campañas de ciberataques patrocinados por Estados y la violencia propia de los conflictos armados[79].

Distinto sería el caso de que, en el curso de un enfrentamiento que efectivamente presente el nivel de violencia de un conflicto armado, se haga uso de herramientas cibernéticas para atacar a la otra parte, tal y como ocurrió en el conflicto entre Georgia y Rusia en 2008 (Schmitt, 2013, pp. 68-69), o en la más reciente invasión rusa sobre Ucrania[80]. Este supuesto, sin embargo, se aleja del objeto del presente trabajo, relativo al impacto sobre el contrato de seguro de las campañas de ciberataques patrocinadas por Estados, valoradas por sí mismas, y no como complemento de otras hostilidades que determinen la existencia de un conflicto armado.

3.2.2. Requisito organizativo

Juntamente con la intensidad, el otro requisito predicable de los conflictos armados alude a la existencia de un grado de organización suficiente como para llevar a cabo acciones violentas de forma continuada por parte de los contendientes. En línea con lo que indicábamos antes, en el caso de las actividades llevadas a cabo por Estados el requisito de la organización se verá satisfecho en la práctica totalidad de los casos. La dificultad principal, pues, residirá en la imputación de un concreto ciberataque a un Estado, especialmente cuando el ataque no sea obra de agentes *de iure* del Estado. Según se ha expuesto, los tribunales emplean alternativamente dos criterios para imputar a un Estado la responsabilidad de una acción ilícita efectuada por sus agentes *de facto*: el del control global y el del control efectivo. Aunque el control efectivo exige un esfuerzo probatorio mayor, en lo que atañe a la determinación de la aplicabilidad de la *exceptio belli* consideramos que el criterio del control global es más apropiado. Según decíamos, la discrepancia entre tribunales se circunscribe al grado de control exigible para imputar responsabilidad a un Estado. Sin embargo, a efectos exclusivamente de determinar la existencia de un conflicto armado (que es precisamente lo aquí nos ocupa), la Corte Internacional de Justicia –principal defensor del requisito del control efectivo– ha reconocido la adecuación del criterio del control global[81].

Por ende, la aplicabilidad de la *exceptio belli* a un ciberataque patrocinado se condiciona a que este se haya llevado a cabo por agentes estatales *de iure* (normalmente personal militar o de inteligencia) o *de facto*. La prueba sobre la asociación entre el Estado y sus agentes

---

79 Aunque el número de víctimas mortales no es *per se* un elemento determinante de la existencia de un conflicto armado, y esta valoración se debe realizar atendiendo a todas las circunstancias que envuelven a los enfrentamientos, debemos recordar que, en la fecha en la que escribimos estas páginas, solo se conoce un único deceso directamente atribuible a un ciberataque, que interrumpió el funcionamiento de un hospital en Alemania (O'Neill y Milutinovic, 2009).

80 Véase el informe elaborado al respecto por Microsoft en 2022. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd

81 Véase *supra* nota 75.

de facto exigirá la demostración de una asistencia (normalmente financiera, de equipamiento, e incluso de recursos de inteligencia) estatal, además de un control general sobre las actividades del grupo[82].

La dificultad de superar este *onus* probatorio constituye el principal obstáculo para la aplicabilidad de la *excepcio belli*. La experiencia práctica[83] demuestra que la identificación de los autores de un ciberataque supone una tarea costosa y compleja, normalmente solo al alcance de las agencias de inteligencia de los Estados afectados que, en el mejor de los casos, suelen hacer valoraciones probabilísticas, estimando un relativo grado de certeza sobre la influencia de un determinado Estado sobre el ciberataque (Banks, 2021, p. 1.052)[84].

En la gran mayoría de los casos, quien pretenda la aplicación de la *exceptio belli* no contará más que con indicios de la asociación entre un Estado y un grupo criminal. La prueba de circunstancias que revelen la existencia de un control global por parte del Estado (tales como el origen de la financiación del grupo o la existencia de comunicaciones que evidencien la intervención del Estado en la planificación de las actividades) se torna, pues, en prácticamente imposible. No obstante, aligerar el *onus probandi* exigiría, como ya se ha discutido, interpretar extensivamente un concepto con efectos restrictivos sobre los derechos del asegurado. En definitiva, el uso de un estándar de atribución más laxo que el del control global implicaría dar la consideración de conflictos armados a situaciones que no serían calificadas como tales de acuerdo con las normas de derecho internacional, sin que existan fundamentos que justifiquen esta divergencia.

3.2.3. Requisito causal

Para la aplicación de la *exceptio belli* no basta con probar la existencia de un conflicto armado. Adicionalmente, los daños cuya exclusión se pretende deben haberse producido por hechos derivados (art. 44 LCS) o producidos (art. 6 TRECCS) por el conflicto armado en cuestión, es decir, debe mediar un nexo causal entre el conflicto y el hecho generador del daño. La relevancia de este requisito se pone de manifiesto por el carácter potencialmente ubicuo de los ciberataques y, más concretamente, por la posibilidad de que los efectos de un conflicto armado se extiendan a terceros Estados que no participan en las hostilidades. Estamos refiriéndonos concretamente al caso del conflicto armado existente a raíz de la invasión rusa sobre Ucrania[85] ya que, coincidiendo con el comienzo de las hostilidades, los

82 *Prosecutor v. Dusko Tadic (Appeal Judgement)*, IT-94-1-A, Tribunal Penal Internacional para la Antigua Yugoslavia (TPIY), 15 de julio de 1999. https://www.refworld.org/cases,ICTY,40277f504.html, para. 130.

83 Véase Banks (2021, p. 1048).

84 Además, en muchas ocasiones, las fuentes de prueba que permiten a un Estado atribuir un ciberataque son secretas, con lo que no pueden ser reveladas al público general.

85 La caracterización de las hostilidades como conflicto armado ha sido reconocida por la gran mayoría de la comunidad internacional. Véase la https://documents-dds-ny.un.org/doc/UNDOC/LTD/N23/048/62/PDF/N2304862.pdf?OpenElement de la Asamblea General de las Naciones Unidas.

ciberataques contra Estados miembros de la OTAN provenientes de grupos asociados a Rusia habrían aumentado de forma drástica[86]. ¿Debe considerarse, pues, que dichos daños han sido provocados por el conflicto armado?

Hay motivos para pensar que, más allá de una correlación, existe una causalidad entre estos ciberataques y el conflicto armado. Sin embargo, no creemos que este nexo posea la intensidad suficiente. El fundamento de la *exceptio belli* reside en que los actos violentos efectuados por grupos dotados la organización suficiente como para llevar a cabo hostilidades de manera relativamente sostenida provocan daños muy extensos en periodos de tiempo concentrados, lo que supone una amenaza de dimensión sistémica para las aseguradoras. Entendiendo el conflicto armado como el conjunto de las hostilidades entre los distintos grupos beligerantes, creemos que la *exceptio belli* no debe amparar más que aquellos siniestros que son resultado directo e inmediato de dichas hostilidades. Esta tesis se ve reforzada por el uso de una interpretación restrictiva de la *exceptio belli* que venimos defendiendo en el presente trabajo. Llevado al caso citado en el párrafo anterior, el hecho de que Rusia participe en un conflicto armado, y que ello le incentive a llevar a cabo ciberataques contra terceros países, no basta para considerar que estos ciberataques hayan sido causados por el conflicto armado, a efectos de la LCS y del estatuto del CCS[87].

Esta conclusión viene respaldada por una de las pocas resoluciones en las que nuestro Alto Tribunal se pronunció sobre las consecuencias de un enfrentamiento bélico sobre el contrato de seguro. En la Sentencia de 10 de enero de 1944, el Tribunal Supremo se pronunció sobre si los actos de robo y saqueo acontecidos en el contexto de la Guerra Civil podían considerarse como siniestros de guerra, entendiendo que no, toda vez que «solo pueden ser considerados siniestros de guerra los que procedan o sean consecuencia directa de operaciones típicamente militares de ataque o defensa»[88]. *Mutatis mutandis*, creemos que la *ratio* de la resolución citada sigue siendo plenamente aplicable; esto es, que los siniestros relacionados con conflictos armados, pero que no son producidos directamente por agresiones entre los partícipes del conflicto no deben quedar amparados por la *exceptio belli*.

En suma, resulta imposible negar de forma categórica la posibilidad de que un ciberataque patrocinado por un Estado pueda ser considerado un evento derivado de un conflicto armado a efectos de su trascendencia sobre un contrato de seguro. Cada ataque es distinto, y podría darse el caso de que, en un futuro, uno o varios ciberataques provocasen los efectos catastróficos propios de un conflicto armado. Sin embargo, en la enorme mayoría de situaciones este no será el caso. Los principales motivos se encuentran en la intensidad de los daños provoca-

---

86 Véase, en este sentido, las conclusiones del informe elaborado por Google en 2023. https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf

87 A menos, claro está, que estos ciberataques, por sí mismos o juntamente con otras agresiones, alcancen la entidad necesaria para entender que existe un nuevo conflicto armado.

88 Cita extraída de Hernando de Larramendi y Caballero García (1972, p. 12).

dos por los ciberataques, que suelen encontrarse (de forma deliberada) por debajo del umbral característico de los conflictos armados, y en la dificultad para atribuir un ciberataque a un Estado concreto. Para los ciberataques que *lato sensu* pueden considerarse como motivados en último término por la existencia un conflicto armado, pero que se dirigen a Estados o grupos que no participan en dicho conflicto (tales como los ciberataques rusos dirigidos contra países distintos de Ucrania), la debilidad del nexo causal entre conflicto y daño constituye, a nuestro parecer, el principal obstáculo para la incluir los siniestros en el ámbito de la *exceptio belli*.

3.3. Breve apunte sobre la terminología empleada en las pólizas

A lo largo de estas páginas hemos estudiado la que nos hemos permitido denominar como *exceptio belli*, tal y como se establece en la LCS y en el TRECCS. Como se ha expuesto, esta exclusión se circunscribe a los daños resultantes de conflictos armados. Sin embargo, dentro del respeto a los límites legales, las aseguradoras privadas son libres de establecer exclusiones distintas, incluidas las relativas a actividades hostiles provenientes de terceros Estados con los que no existe una situación de conflicto armado. A nivel internacional, en noviembre de 2021 el Lloyd's of London hizo públicas cuatro posibles cláusulas[89] a incluir en las pólizas de ciberseguros suscritas por sus sindicatos, en las que se excluían los daños causados por «ciberoperaciones»[90]. La Asociación de Ginebra, *think tank* que reúne a las principales (re) aseguradoras del mundo, hizo públicos en 2020 tres informes en los que se proponía el uso del término de «ciberactividad hostil» (Geneva Association, 2020, pp. 14 y ss.) precisamente para tratar de solventar las fricciones que se producen al tratar de subsumir los ciberataques patrocinados por Estados dentro de las categorías clásicas de violencia interestatal. En nuestro país, resulta común que en las pólizas de ciberseguros se excluyan los daños causados por «actos de enemigos extranjeros», «hostilidades» u «operaciones de guerra».

Cada una de estas categorías tendrá sus propios límites y problemáticas, que trascienden el objeto de este trabajo. Bástenos con añadir dos breves notas interpretativas: la primera, que para los contratos de seguro celebrados entre partes que no se sitúen en un plano de igualdad[91], las exclusiones de hostilidades distintas de los conflictos armados tendrán carácter limitativo sobre los derechos del asegurado, con lo que deberán destacarse de modo especial, de acuerdo con el mandato del artículo 3 de la LCS, no pudiendo beneficiar las ambigüedades en las exclusiones a la parte que hubiese ocasionado la oscuridad. La segunda

89 Disponibles en https://www.lmalloyds.com/LMA/News/LMA_bulletins/LMA_Bulletins/LMA21-042-PD.aspx

90 Definidas como «el uso de un sistema informático por o por cuenta de un Estado para interrumpir, denegar, degradar, manipular o destruir información en un sistema informático de otro Estado, o localizado en otro Estado» (traducción propia).

91 Con esto nos estamos refiriendo a la exclusión del carácter imperativo de la LCS que efectúa el artículo 44.2 para los seguros de grandes riesgos, tal y como se definen en el artículo 11 de la Ley 20/2015, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras.

es que, en contraste con lo anterior, la defensa de una interpretación estricta de las cláusulas que limiten la resarcibilidad de los siniestros encuentra como límite necesario el respeto a la literalidad de lo pactado de forma lícita, ya que *in claritas non fit interpretatio*.

4. Conclusión

Mediante este trabajo hemos pretendido examinar el posible impacto de los ciberataques patrocinados por Estados sobre el contrato de seguro. Dado un ciberataque patrocinado del que se deriven efectos dañosos sobre intereses asegurados mediante póliza privada, y siempre que concurran los demás requisitos a los que la ley condiciona la cobertura del CCS (aseguramiento mediante una póliza de un ramo para el que se exija el pago del recargo pertinente, transcurso del periodo de carencia, etc.), serán los indicios sobre la finalidad perseguida mediante el ataque (y, particularmente, si dicha finalidad es o no terrorista) los que determinen si por los daños debe responder la aseguradora privada o el Consorcio de Compensación de Seguros, en los términos descritos en su normativa reguladora. En cualquiera de los dos casos, la concurrencia de un elemento bélico puede eximir de responsabilidad a la aseguradora privada o al CCS.

No obstante, no creemos que las exclusiones de los daños producidos por conflictos armados contempladas en la LCS y en el TRECCS sean aplicables a la inmensa mayoría de ciberataques patrocinados. De una parte, porque no resulta sencillo que estos ataques alcancen por sí mismos el nivel de intensidad en la violencia que caracteriza a los fenómenos que típicamente se designan como conflictos armados. De otra, porque la dificultad de probar la autoría del Estado patrocinador complica aún más la aplicación de la excepción a la que nos venimos refiriendo.

De acuerdo con nuestro estudio, resulta imposible ofrecer una respuesta categórica sobre la cobertura de los ciberataques patrocinados por Estados. Dicha simplificación obviaría las diferencias entre una estafa a un particular perpetrada por un grupo que opera impunemente en fronteras chinas y los ataques llevados a cabo por Rusia contra infraestructuras ucranianas como parte de su campaña militar. Así, será la evaluación conjunta de los elementos que caracterizan cada ciberataque patrocinado la que determinará su calificación jurídica.

Sin embargo, dicha calificación puede encontrar dificultades infranqueables en no pocos casos. Esto se debe a que elementos relevantes a la hora de subsumir un ataque dentro de una categoría jurídica u otra (tales como la motivación perseguida o el nexo que vincula al grupo agente con el Estado patrocinador) pueden llegar a ser imposibles de probar, por motivos geográficos o tecnológicos. Quizás este trabajo permita iniciar un debate sobre la necesidad de replantear el sistema español de cobertura de los eventos extraordinarios, incorporando nuevas categorías que se adecuen a un nuevo paradigma que supere la separación tajante de guerra y paz, y en el que las hostilidades cibernéticas no sean sino otro elemento integrante de la diplomacia internacional.

Referencias bibliográficas

Banerjea, A. (2018). NotPetya: How a Russian malware created the world's worst cyber-attack ever. *Business Standard*. https://www.business-standard.com/article/technology/notpetya-how-a-russian-malware-created-the-world-s-worst-cyberattack-ever-118082700261_1.html

Banks, W. (2021). Cyber Attribution and State Responsibility. *International Law Studies*, *97*. https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=2980&context=ils

Barrero Rodríguez, E. (2000). *El Consorcio de Compensación de Seguros*. Tirant lo Blanch.

Bing, C. y Kelly, S. (2021). Cyber attack shuts down U.S. fuel pipeline 'jugular,' Biden briefed. *Reuters*. https://www.reuters.com/technology/colonial-pipeline-halts-all-pipeline-operations-after-cybersecurity-attack-2021-05-08/

Bonhome González, C. (2010). El Consorcio de Compensación de Seguros. En P. Blanco-Morales (Ed.), *Estudio sobre el sector asegurador en España* (pp. 213-235). Fundación de Estudios Financieros.

Caamaño Malagón, J. (2022). ¿Cómo funcionan los seguros en caso de guerra? Un recorrido por la Historia. *Mapfre*. https://www.mapfre.com/actualidad/seguros/como-funcionan-seguros-en-caso-de-guerra/

Centro Criptológico Nacional. (2021). Principios y recomendaciones básicas en Ciberseguridad. CCN-CERT. https://www.ccn-cert.cni.es/informes/informes-de-buenas-practicas-bp/2473-ccn-cert-bp-01-principios-y-recomendaciones-basicas-en-ciberseguridad/file.html

Comité Internacional de la Cruz Roja. (2008). ¿Cuál es la definición de «conflicto armado» según el derecho internacional humanitario? Comité Internacional de la Cruz Roja. https://www.icrc.org/es/doc/assets/files/other/opinion-paper-armed-conflict-es.pdf

Consorcio de Compensación de Seguros. (2018). La cobertura de los riesgos extraordinarios en España. https://www.consorseguros.es/web/documents/10184/35211/Cobertura_Riesgos_Extraordinarios/7c2721bf-890b-435c-8ffa-8c2a58fc664d

Cooper, J. (2022). Demystifying Common Clauses. *Marsh*. https://www.marsh.com/na/industries/energy-and-power/insights/energy-power-newsletter-q4-2021/demystifying-common-clauses-q4-2021.html

Council on Foreign Relations. (s. f.). Cyber Operations Tracker. https://www.cfr.org/cyber-operations/#Map

David, E. (2008). *Principes de droit des conflits armés*. Bruylant.

ENISA. (2022). ENISA Threat Landscape 2022. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

García Barona, A. (1997). El Consorcio de Compensación de Seguros y los Riesgos Catastróficos. *V Congreso Iberoamericano de Derecho de Seguros* (tomo 2, pp. 401-411).

Geneva Association. (2020). Cyber War and Terrorism: Towards a common language to promote insurability. The Geneva Association. https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public/cyber_war_terrorism_commonlanguage_final.pdf

Giménez, Ó. (2020). La banca impulsa la venta de ciberseguros a las pymes con la crisis del coronavirus. *El Confidencial*. https://www.elconfidencial.com/empresas/2020-05-11/banca-ciberseguros-pymes-teletrabajo-hackers-coronavirus_2586599/

González de Frutos, P. (1993). El Reglamento de Riesgos Extraordinarios. https://documentacion.fundacionmapfre.org/documentacion/publico/es/media/group/1030644.do

Greenberg, A. (2018). The Untold Story of NotPetya, the Most Devastating Cyberattack in History. WIRED. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Henckaerts, J. M. y Comité Internacional de la Cruz Roja. (2016). Commentary on the First Geneva Convention: Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (L. Lijnzaad, M. Sassòli, J.-M. Henckaerts, P. Spoerri, & K. Dörmann, Eds.). Cambridge University Press.

Hernando de Larramendi, I. y Caballero García, A. I. (1972). El Seguro y los actos de violencia cometidos contra una comunidad y que causan lesiones a personas y daños materiales: ponencia de la Sección Española de la A.I.D.A. *IV Congreso Mundial de Derecho de Seguros.*

Horrillo Muñoz, M. Á., Soriano Cavero, B. y Espejo Gil, F. (2020). Análisis de la siniestralidad de los riesgos extraordinarios del Consorcio de Compensación de Seguros 1995-2019. *Consorseguros*, *13*, 4-18.

Insikt Group. (2019). The History of Ashiyane: Iran's First Security Forum. Recorded Future. https://www.recordedfuture.com/ashiyane-forum-history

Jimeno Muñoz, J. (2019). Los ciber seguros y los efectos de los ciber riesgos en los seguros de responsabilidad civil. En *Derecho de daños tecnológicos, ciberseguridad e insurtech* (pp. 125-267). Dykinson.

Kaczorowska, A. (2015). *Public International Law*. Routledge.

Kovacs, E. (2018). U.S., Canada, Australia Attribute NotPetya Attack to Russia. *SecurityWeek*. https://www.securityweek.com/us-canada-australia-attribute-notpetya-attack-russia/

Lilly, B. y Cheravitch, J. (2020). The Past, Present, and Future of Russia's Cyber Strategy and Forces. *International Conference on Cyber Conflict (CyCon)*, *12*, 129-155.

Martin, A. (2022). Mondelez and Zurich reach settlement in NotPetya cyberattack insurance suit. *The Record by Recorded Future*. https://therecord.media/mondelez-and-zurich-reach-settlement-in-notpetya-cyberattack-insurance-suit

Mazzuoli, V. d. O. (2017). *Derecho internacional público contemporáneo* (H. T. Baires Flores, trad.). Editorial Cuscatleca.

Microsoft. (2022). Microsoft Digital Defense Report 2022. Microsoft. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bUvv?culture=en-us&country=us

Mosquera Blanco, A. J. (2022). La definición de terrorismo tras la Ley Orgánica 2/2015, de 30 de marzo. *Cuadernos de Política Criminal. Segunda Época*, *138*, 199-243.

National Institute of Standards and Technology. (2019). Cyber Attack - Glossary | CSRC. NIST Computer Security Resource Center. https://csrc.nist.gov/glossary/term/cyber_attack

O'Connell, M. E. y Gardam, J. (2010). Final Report on the Definition of Armed Conflict in International Law. https://www.rulac.org/assets/downloads/ILA_report_armed_conflict_2010.pdf

O'Neill, P. H. y Milutinovic, A. (2009). Tecnología y Sociedad. Una persona fallece a causa de un ciberataque por primera vez en la historia. *MIT Technology Review*. https://www.technologyreview.es//s/12647/una-persona-fallece-causa-de-un-ciberataque-por-primera-vez-en-la-historia

OECD. (2021). Enhancing financial protection against catastrophe risks: the role of catas-

trophe. OECD. https://www.oecd.org/daf/fin/insurance/Enhancing-financial-protection-against-catastrophe-risks.pdf

Pastrana Sánchez, M. A. (2020). *La nueva configuración de los delitos de terrorismo*. Agencia Estatal Boletín Oficial del Estado.

Peralta, L. A. (2022). Así es Conti, la banda de hackers que extorsiona países enteros. *Retina*. https://retinatendencias.com/tech-society/asi-es-conti-la-banda-de-hackers-que-extorsiona-paises-enteros/

Perlroth, N. (2019). Big Companies Thought Insurance Covered a Cyberattack. They May Be Wrong. (Published 2019). *The New York Times*. https://www.nytimes.com/2019/04/15/technology/cyberinsurance-notpetya-attack.html

Pictet, J. (1952). Commentary on the Geneva Conventions of 12 August 1949, vol. 1. *Geneva Convention for the Amelioration of the Wounded and Sick in Armed Forces in the Field*.

Sánchez Calero, F. (Dir.). (2010). *Ley de Contrato de Seguro. Comentarios a la Ley 50/1980, de 8 de octubre, y a sus modificaciones*. Aranzadi.

Sanger, D. E. (2012). Obama Ordered Wave of Cyberattacks Against Iran. *The New York Times*. https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html

Scherschel, F. A. (2016). Petya, Mischa, Goldeneye: Die Erpresser sind Nerds. *Heise*. https://www.heise.de/newsticker/meldung/Petya-Mischa-Goldeneye-Die-Erpresser-sind-Nerds-3571937.html

Schmitt, M. N. (Ed.). (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press.

Schwindt, K., Ma, L., Marcinek, K. y Hodgson, Q. E. (2019). Fighting Shadows in the Dark: Understanding and Countering Coercion in Cyberspace. RAND Corporation.

Tirado Suárez, F. J. (1995). El seguro privado y los actos terroristas en Derecho Español. En *Estudios de Derecho Mercantil en homenaje al profesor Manuel Broseta Pons* (tomo III, pp. 3.767-3.803). Tirant lo Blanch.

Wolff, J. (2022). Who Will Pay the Price for Cyberattacks? *The Wall Street Journal*. https://www.wsj.com/articles/who-will-pay-the-price-for-cyberattacks-11662645501

Ignacio Sánchez Gil. Graduado en Derecho y ADE por el Instituto de Empresa, y doctorando en el Departamento de Derecho Mercantil de la Universidad Complutense de Madrid, donde trabaja en su tesis relativa a los vicios de las modificaciones estructurales de las sociedades mercantiles. Ignacio ha publicado trabajos sobre distintos temas tales como la responsabilidad de las plataformas *online* o la aplicabilidad de la normativa financiera a los criptoactivos en revistas como la *Revista de las Cortes Generales*, la *Revista General de Derecho de los Sectores Regulados* o *Telos*. En cuanto a su trayectoria profesional, ha trabajado en el despacho de abogados Andersen, especializándose en protección de datos y ciberseguridad. https://orcid.org/0000-0003-0130-1350