La creciente necesidad de legislación contra las amenazas cibernéticas, fuentes de graves daños transnacionales*

The growing need for legislation against cyber threats, sources of serious transnational harm

A María de los Ángeles, mi mujer,
porque sin ella ni este (el último trabajo…)
ni ningún otro, tampoco,
de los muchos cuya publicación he conseguido
a lo largo de estos años hubiera visto la luz.

Cesáreo Gutiérrez Espada
Catedrático Emérito de Derecho Internacional Público y Relaciones Internacionales
Universidad de Murcia

Recibido: 03.05.2022 / Aceptado: 23.05.2022
DOI: 10.20318/cdt.2022.7169

Resumen: Las amenazas cibernéticas son una creciente fuente de preocupación. Y más aún lo es la práctica actual de los ciberataques.Tanto en Estados Unidos como en la Unión Europea, conscientes del problema, han iniciado la adopción de medidas normativas que buscan una mejor protección contra los diversos tipos de ataques cibernéticos.Entre dichas medidas, se baraja incluso la adopción de contramedidas o represalias contra los autores de dichos ataques.

Palabras clave: Amenazas cibernéticas,Congreso de los Estados Unidos, contramedidas como respuesta a ciberataques,infraestructuras críticas, Manual de Tallinn 2.0,Senado de los Estados Unidos, Unión Europea.

Abstract: Cyber threats are a growing source of concern. And even more so is the current practice of cyber attacks. Both the United States and the European Union, aware of the problem, have begun to adopt regulatory measures that seek better protection against the various types of cyber attacks. Among these measures, even the adoption of countermeasures or retaliation against the perpetrators of such attacks is considered.

Keywords: Cyber threats, United States Congress, countermeasures in response to cyber attacks, critical infrastructure, Tallinn Manual 2.0, United States Senate, European Union.

* Esta publicación es resultado del Proyecto de I+D+i en el marco de los programas estatales de generación de conocimiento y fortalecimiento científico y tecnológico del sistema de I+D+i y de I+D+i orientada a los Retos de la Sociedad, convocatoria 2020, Proyecto PID2020-112577RB-I00 ("La búsqueda de una regulación internacional para las actividades cibernéticas, ¿una ineludible necesidad?"), financiado por MCIN/ AEI /10.13039/501100011033.

I. Las amenazas cibernéticas en la práctica actual

1. Actividades cibernéticas maliciosas contra la sociedad civil

1. Hoy en día los dispositivos electrónicos forman parte importante de nuestras vidas y nos cuesta imaginar que podamos prescindir de ellos.

Esta dependencia explica, en buena parte al menos, el por qué los estudios y, después, las profesiones en seguridad cibernética están creciendo tanto. Los puestos de trabajo en seguridad de la información, el desarrollo webs y la llamada arquitectura de redes han subido en torno a un 25% en los últimos 5 años

Claro que también han aumentado los ataques (…).

2. El Mando Conjunto del Ciberespacio es el de más reciente creación dentro del ejército español, pero cada vez cobra más relevancia, porque a medida que avanzan las nuevas tecnologías, también lo hacen, sí, los ciberataques[1]. Si algo nos ha enseñado la pandemia que sufrimos es que la amenaza más peligrosa, a veces invisible, puede, por sus consecuencias, paralizar, íntegramente, un país. Esto sucede, precisamente, con los ciberataques.

Fuentes del Mando Conjunto del Ciberespacio alertan de que España es el tercer país del mundo que sufre más ciberataques. Estos proceden de organizaciones criminales (asociadas o no a un Estado) cada vez más profesionalizadas, siendo muy difícil atribuir su autoría.

Pero, ¿quién puede sufrir un ciberataque? Desde una centrifugadora nuclear, hasta el GPS de un barco o el sistema informático de un hospital del que pueden depender cientos de vida. Según la Organización del Tratado del Atlántico Norte (OTAN), el ciberespacio ya es el quinto dominio de operaciones militares, y, como tal, debemos estar preparados para hacer frente a los conflictos que se libran en él y desde él.

Y para eso hay que entrenarse. Del mismo modo que los soldados del Ejército de Tierra ensayan sus operaciones en campos de maniobras, o los marinos en una fragata, los efectivos del Mando Conjunto del Ciberespacio lo hacen en simulacros virtuales. Hay dos ejercicios claves cada año, uno a nivel nacional y otro internacional organizado por la OTAN; el *Cyber Coalition,* es el ejercicio de ciberdefensa colectiva insignia de esta Organización. Viene realizándose desde 2008 (con la participación de España), tratándose de un ejercicio con tres objetivos clave:

— Ejercer los mecanismos existentes para la interacción entre la OTAN, sus aliados y socios, a fin de mejorar la colaboración en el ámbito del ciberespacio
— Perfeccionar la capacidad de la Alianza para realizar operaciones en el ciberespacio, por medio de entidades civiles y militares, mediante el intercambio de inteligencia de este ámbito y la gestión de incidentes cibernéticos.
— Y proporcionar información que desvele posibles brechas de seguridad, requisitos de capacitación y validar procedimientos en desarrollo para apoyar el buen funcionamiento de la guerra cibernética.

Los escenarios de 2021 incluyeron un ciberataque a las tuberías de suministro de gas de un país ficticio; otro, que interrumpía el despliegue de tropas y la logística; y un ataque de *ransomware* (*vid. nfra* nota 9) relacionado con una pandemia, en el que se robaban datos de vacunas y se ponían en peligro los programas de vacunación.

[1] M.Senovilla, "El Mando Conjunto del Ciberespacio ha contenido más de 600 ataques peligrosos para la defensa de España en el último año", 26 de enero de 2022 (https://atalayar.com)

Escenarios, éstos, menos ficticios de lo que cabría imaginar. Recuérdese el ciberataque masivo sufrido por Ucrania no hace mucho tiempo que inhabilitó los sitios web de su Ministerio de Asuntos Exteriores, además de lanzar un mensaje con el fin de desatar el pánico de los ciudadanos (por si el estar inmersos en la escalada de tensión ante los movimientos de Rusia, no fuera bastante…). Escribirlo precisamente en estos días, no pocos ya, desde la invasión de Ucrania por tropas rusas (un jueves, 24 de febrero de 2022), puede resultar irónico (...).

3. Comprender las amenazas cibernéticas resulta indispensable para defendernos de ellas. Pensemos un poco en los desafíos más relevantes, también, sin duda, los más corrientes o elementales, en este ámbito.

La mayoría de los usuarios no son conscientes de los riesgos que existen al utilizar su teléfono inteligente o su tablet en redes sociales como WhatsApp, Facebook, Twitter (...), instalarse cada dos por tres aplicaciones de entretenimiento, "bajarse" aplicaciones bancarias, "visitar" webs de pornografía o realizar descargas piratas de películas, música o juegos que, muchas veces, van acompañados de *malware* (código maligno) que se alojará en sus dispositivos.

Los *malwares* ralentizan la velocidad de la máquina, roban su información o atacan infraestructuras relevantes para la vida de un país. A través del *malware*, los *hackers* controlan ordenadores, teléfonos o *tablets* de los usuarios y vigilan sus movimientos para, entre otros fines, descubrir las contraseñas que han introducido. Pero eso es lo menos dañino, ya que en el peor de los casos se alojan en las "máquinas" "virus" que graban lo que el usuario hace y toman el control de su ordenador para cometer delitos económicos o atacar redes y sitios web; esta configuración es conocida red de *bots*. Lo peor de todo es que existe una amplia posibilidad de que el cibernauta contamine a sus conocidos y contactos con su correo. Diseminar *malware* en sitios de redes sociales es algo que está creciendo a un ritmo alarmante; y es que aunque aquellos cuentan con sistemas para minimizar los riesgos, los creadores de *malware* también tienen mucha práctica y una más que demostrada mala fe.

Una forma común para obtener el control de la información personal de los clientes es a través de delitos informáticos como el *phishing*. Mediante esta técnica, los ciberdelincuentes crean un correo que parece generado por una empresa legítima. En él, se solicita información personal del destinatario del correo (su número de cuenta o clave de acceso, por ejemplo) para, luego, utilizar los datos obtenidos para cometer delitos económicos, obtener tarjetas de crédito fraudulentas a nombre de un consumidor o, en fin, generar gastos importantes que, naturalmente, deberá pagar el afectado. Fraudes de este tipo tienen éxito en no pocas ocasiones, ya que en ellos se emplean técnicas de ingeniería social para ganarse la confianza del usuario.

Cuando contratamos un servicio de línea telefónica o acceso a Internet para la casa, acude normalmente un técnico quien deja el dispositivo funcionando y le pone una clave de acceso antes de retirarse. Sin embargo, hoy existen herramientas gratuitas que cualquiera puede bajar de Internet y sirven para "romper" claves sencillas. Si usted está en alguno de estos supuestos, se podrá entrar en su red personal y observar toda la información que pasen por el tubo de comunicación; y si usted suele consultar su saldo o hacer compras o realizar operaciones en el banco por Internet, existe una alta posibilidad de que albergue en su casa un inquilino indeseable que utilizará toda esa información para hacerse con su dinero.

Los accesos en parques públicos, quioscos y aeropuertos son de lo más vulnerable que se puede imaginar. Para el *hacker*, un aeropuerto es el cuerno de la abundancia: puede encontrar ejecutivos, empresarios o personas con tarjetas de crédito accediendo a sus bancos, comprando por Internet o abriendo sus cuentas de correo… Los ordenadores en los cibercafés son una posible trampa si un *hacker* deja instalado un *spyware* en los dispositivos instalados. Y lo mismo ocurre cuando te conectas a una red desconocida: en apariencia encontrar una conexión gratis es una suerte, pero todas las conexiones inalámbricas que existen tienen su lado oscuro (…).

4. Este recorrido elemental por las principales técnicas cibernéticas "maliciosas" pretende dejar claro, desde el principio, las eventuales consecuencias de su utilización.

El lector podrá imaginarse mejor, así, el panorama que generaría su empleo contra determinadas infraestructuras de un Estado. Volveré sobre ello enseguida.

2. Actividades cibernéticas maliciosas contra Estados o sus intereses

5. Pero las actividades maliciosas o ilícitas, como las comentadas *supra* (párrafo 3), que se llevan a cabo en el ciberespacio, no solo tienen que ver con la comisión de delitos contra las personas (y sus bienes) que habitan un país, esto es, la cibercriminalidad[2], sino que pueden desarrollarse en el plano genuinamente internacional, en el de las relaciones entre Estados soberanos o, más ampliamente, entre sujetos del Derecho internacional.

6. Así, esas actividades cibernéticas pueden utilizarse por un Estado (o un grupo privado incluso) para espiar a otro Estado o sujeto de Derecho internacional.

> "El ciberespionaje es un método relativamente económico y rápido y con menos riesgo que el espionaje tradicional, dada la dificultad de atribución de la autoría [3].

7. Asimismo, se percibe en la actualidad una tendencia creciente de las denominadas amenazas híbridas. Esto es, en palabras de la Estrategia española de Ciberseguridad de 2019:

> "acciones coordinadas y sincronizadas dirigidas a atacar de manera deliberada las vulnerabilidades sistémicas de los Estados democráticos y sus instituciones, por medio de una amplia gama de medios, tales como acciones militares tradicionales, ciberataques, operaciones de manipulación de la información o elementos de presión económica"[4]

8. Los grupos terroristas tratan de aprovechar las características del ciberespacio para cometer ciberataques o llevar a cabo actividades de radicalización de individuos y colectivos, financiación, divulgación de técnicas e instrumentos para la comisión de atentados, y de reclutamiento, adiestramiento o propaganda[5].

9. Íntimamente relacionadas con ello están las amenazas contra las infraestructuras críticas del Estado, con la posibilidad de causar un colapso a través de las redes y mediante una caída en cadena de los servicios esenciales[6].

Volveré sobre esta cuestión después (párrafos 22-23 y 36-37).

3. Algunos ejemplos de la práctica internacional relativos al desarrollo malicioso de actividades cibernéticas

A) En los Estados Unidos

10. El proveedor informático *SolarWinds* hizo público, en diciembre de 2020, „que sus sistemas sufrieron un ataque manual altamente sofisticado a la cadena de suministros de su *software* Orion". Un ciberataque „extremadamente dirigido" que habría sido obra de "un Estado nacional externo".

No es un objetivo sin importancia, precisamente, pues entre los clientes de *SolarWinds* se encuentran la mayoría de grandes empresas de los Estados Unidos, además de organizaciones guberna-

[2] La Estrategia española en este tema, distingue, en función del hecho punible en sí (de la autoría, de su motivación o de los daños infligidos) tres clases de cibercrimenes: ciberterrorismo, ciberdelito y hacktivismo (*Estrategia Nacional de Ciberseguridad 2019*, Departamento de Seguridad Nacional, Presidencia del Gobierno, Gobierno de España, 2019, pp. 1-136, p. 25).

[3] *Ibidem,* p. 25.

[4] *Ibidem.* Como, en un caso de la práctica actual, la guerra en Ucrania (*vid. ad ex.* CUBEIRO CABELLO, E., "El ciberespacio en la guerra de Ucrania", *Documento de Opinión* (Instituto Español de Estudios Estratégicos, IEEE), 32/2022, 4 de abril de 2002, pp. 1-14,

[5] *Estrategia Nacional de Ciberseguridad 2019*, *op. cit*. (nota 2 *supra*), p. 26.

[6] *Ibidem.*

mentales como la Administración Nacional de Aeronáutica y del Espacio (NASA), las fuerzas aéreas o el Pentágono.

Fuentes del *Washington Post* apuntaron a Rusia como origen del ciberataque.

El sistema Orion es una herramienta de monitorización y administración de redes, utilizado por muchas grandes empresas. Se cree que, en la actualización del mes de marzo (2020), se habría introducido una "puerta trasera", comprometiendo la herramienta Orion y de paso toda la infraestructura de las empresas que lo utilizan.

Por parte de *Microsoft* también se confirmó el ataque a Orion. La compañía creía que:

> "se trata de una actividad de Estado-nación a una escala significativa, dirigida tanto al gobierno como al sector privado"[7].

11. El operador del oleoducto *Colonial Pipeline*[8], que se extiende desde Texas hasta Nueva Jersey, cerrado tras sufrir un ataque cibernético de *ransomware*[9], declaraba, el 10 de mayo de 2021, que esperaba reiniciar la mayoría de sus operaciones en unos días.

Colonial Pipeline detuvo los envíos al parecer como medida de precaución para evitar que los piratas informáticos adoptasen medidas adicionales, vga. apagar o dañar el sistema.

El ataque, realizado según la Oficina Federal de Investigaciones (FBI) por un grupo de crimen organizado llamado *DarkSide*, puso de manifiesto la vulnerabilidad del sistema de energía estadounidense.

Este oleoducto tiene su sede en Alpharetta (Georgia) y es uno de los más extensos de Estados Unidos. Puede transportar alrededor de 3 millones de barriles de combustible al día a través de 8.850 kilómetros, de Houston a Nueva York. Da servicio a la mayoría de los Estados del Sur y tiene ramific - ciones en la costa Atlántica, hasta Tennessee. Es crítico, en particular, para el funcionamiento de muchos aeropuertos del este de Estados Unidos.

En la actualidad, el oleoducto *Colonial*, que es privado, pertenece a Royal Dutch Shell, Koch Industries y varias firmas de inversión extranjeras y estadounidenses

12. *Netwalker* es un tipo de *ransomware* que se dio a conocer en septiembre de 2019, aunque ganó notoriedad en marzo de 2020, cuando no pocos Estados comenzaron a decretar confinamientos por el Covid-19[10].

Este *ransomware*, cuya creación se atribuye al grupo ruso *Circus Spider,* y tras lo que aparentemente fueron ensayos para probar su eficacia, pasó a funcionar como un *ransomware as a service* (RaaS), en el que el grupo desarrollador del *malware* ofrecía, a través de la *dark web*, un sistema de afiliación para utilizarlo y propagarlo entre diferentes objetivos, a cambio de quedarse con un porcentaje del rescate.

Para afiliarse a *NetWalker*, y además de tener las capacidades que exigían sus creadores, debían cumplirse otra tipo de reglas (por ejemplo, no atacar organizaciones ubicadas en Rusia o en la Comunidad de Estados Independientes[11]; debiéndose devolver, asimismo, los archivos robados a las víctimas, una vez pagado el rescate).

---

[7] E.Pérez, "Un sofisticado ciberataque contra *SolarWinds* enciende las alarmas: el proveedor del Pentágono y decenas de grandes compañías ha sido comprometido", 14 de diciembre 2020 (https://www.kataka.com).

[8] C.Krauss, "Ciberataque al oleoducto Colonial Pipeline: esto sabemos" 11 de mayo de 2021, (https://www.nytimes.com/es/2021/05/11/espanol/colonial-pipeline-ransomware.html).

[9] Un *ransomware***,** del inglés *ransom*, 'rescate', y *ware*, acortamiento de *software*, o "secuestro de datos" en español, es un tipo de programa dañino que restringe el acceso a determinadas partes o archivos del sistema operativo infectado y pide un rescate a cambio de quitar esta restricción.

[10] H. Ramírez, "NetWalker, el *ransomware* que se aprovechó del Covid-19 para atacar centros educativos y de salud", 26 de julio de 2021 (https://www.protecciondatos-lopd.com).

[11] "Organización internacional subregional surgida tras la disolución de la Unión Soviética con la finalidad de preservar los lazos políticos y económicos entre varias repúblicas exsoviéticas y contribuir a la realización de la democracia, la protección de los derechos humanos y la transición hacia la economía de mercado. Se creó en diciembre de 1991 mediante los acuerdos de Minsk y Alma-Ata, completados con la Carta de la CEI de 22 de enero de 1993. Algunos de sus Estados miembros han constituido agrupaciones subregionales dentro de la CEI" ("Comunidad de Estados Independientes", *Diario panhispánico del español jurídico*, https://dpej.rae.es)

Como otras modalidades de *malware*, *NetWalker* se distribuye por correo electrónico, mediante campañas masivas de *emails* fraudulentos, que en muchos casos lleva archivos adjuntos con supuesta información sobre el Covid-19.

Una vez ha infectado un equipo, *NetWalker* puede propagarse con relativa facilidad a otros conectados a la misma red de Windows en la que esté el equipo infectado originalmente.

Los primeros ataques de *NetWalker* se centraron en usuarios particulares, con demandas de rescates no muy elevadas (si las comparamos a las que se piden cuando el objetivo es una gran empresa), pero a partir de marzo-abril de 2020, los objetivos de este tipo de cibercriminales cambiaron, pasando a ser atacadoss objetivos mayores, a los que podían demandarse cantidades muy superiores de dinero.

Entre estos objetivos nuevos, empresas privadas, hospitales, organismos públicos y centros educativos. Una vez en la red pretendida, sus autores cifran los archivos y envían la carta de rescate para exigir una cantidad de dinero determinada a cambio de la clave de desencriptado.

El *ransomware NetWalker* ha sido uno de los más activos y de los que ha sabido aprovechar mejor las carencias en materia de ciberseguridad en momentos álgidos de la pandemia. Algunas de las organizaciones atacadasas por *NetWalker* fueron:

— El sistema de salud *Crozer-Keystone* de Filadelfia (cuatro hospitales y varios centros de salud) sufrió un ciberataque de este tipo a mediados de junio de 2020.
— El Hospital Universitario de Brno, en la República Checa, fue atacado en marzo de 2020, retrasando los resultados de las pruebas de Covid que se procesaban allí.
— En España varios hospitales fueron víctimas de *NetWalker*, también en marzo de 2020.
— La Universidad Estatal de Michigan, la Universidad de Columbia en Chicago o la de California en San Francisco resultaron, igualmente, quedaron afectadas por este *ransomware*.
— La ciudad austriaca de Weiz fue, asimismo, uno de los objetivos de *NetWalker* en mayo de 2020, que logró introducirse en la red pública de la ciudad.
— La Dirección Nacional de Migraciones de Argentina fue, asimismo, atacada porn *NetWalker* en septiembre de 2020, lo que obligó a desconectarla de la red durante un tiempo, para frenar la propagación del virus.

Como buena noticia, el Departamento de Justicia de Estados Unidos, en colaboración con autoridades búlgaras, anunció el inicio de acciones para detener este *ransomware*, identificar y procesar a sus autores y recuperar los pagos de las víctimas. El Departamento de Justicia, en efecto, hizo pública formalmente[12] una acción coercitiva coordinada con base en el Derecho internacional, para poner fin (*disrupt*) al *NetWalter ransomware*[13].

En marzo de 2021, se habría producido una primera detención; la de un ciudadano canadiense acusado de haber ganado 27,6 millones de dólares con ciberataques de *NetWalker*.

13. La conocida compañía estadounidense *Microsoft Exchange* advirtió a miles de sus clintes, en agosto de 2021, algunas de las empresas más grandes del mundo, que un grupo de ciberdelincuentes había podido acceder a sus cuentas y contarían, probablemente, con la capacidad de leer, cambiar o incluso eliminar sus principales bases de datos[14]. La vulnerabilidad se localizó, tal y como se desprende de la copia de un correo electrónico y de la opinión de un investigador de seguridad cibernética, en la base de datos insignia Cosmos DB de Microsoft Azure, de lo que se hizo eco la agencia Reuters.

Un equipo de investigación de la empresa de ciberseguridad *Wiz* descubrió que podía acceder a las claves que controlan el acceso a las bases de datos de miles de empresas, según explicó Ami Luttwak, Directora de Tecnología de *Wiz*.

[12] *The United States Department of Justice*, January 27, 2021.

[13] J.Panettieri, "U.S. Cybersecurity Strategy: President Biden Executive Orders, Legislation, Leaders and More", pp.1-4, p. 2 (https://www.msspalert.com/cybersecurity-markets/americas).

[14] C.Ferrer-Bomsoms Cruz, "Microsoft avisa a miles de clientes de su nube de que sus bases de datos están expuestas por un grave fallo de seguridad", 27 de agosto de 2021, (https://www.businessinsider.es)

La compañía de Redmond no puede cambiar las claves de sus clientes, por lo que envió un correo electrónico a los afectados indicándoles, para evitarse problemas, que debían crear nuevas contraseñas.

La Directora de Tecnología de *Wiz* hizo, asimismo, público que los clientes que no recibieron ningún correo de Microsoft también habían podido verse afectados, por lo que les recomendaba, igualment, el cambio de contraseñas.

14. Y en el ámbito de las infraestructuras críticas, también la Autoridad Metropolitana de Transporte (MTA) de Nueva York fue objeto de ataques, en abril de 2021, a sus sistemas informáticos[15].

B) En la Unión Europea

15. Diversos Estados miembros de la Unión y algunas de sus instituciones han sido blanco de actividades informáticas malintencionadas en los últimos años.

Más aún, los ciberataques contra sectores críticos en Europa se duplicaron en 2021, con la expansión de la digitalización que generó la pandemia, y teniendo su origen la mayoría de ellos (como en tantos otros casos) en Rusia.

Aunque desde las instituciones de la Unión Europea se tomaron medidas para minimizar sus efectos, el conflicto armado en Ucrania no ha hecho más que intensificar la ciberguerra e incitar a los ciberdelincuentes. Solo en 2020 (aún no hay datos oficial s ciertos de 2021), se gestionaron un total de 133.155 incidentes de ciberseguridad desde el Instituto Nacional de Ciberseguridad (Incibe)[16].

16. Así, la Agencia Europea del Medicamento (EMA), que denunció, el miércoles 16 de diciembre de 2020, haber sido objeto de un „ciberataque", informaba de la apertura „inmediata de una investigación" en colaboración con la policía holandesa, puesto que su sede se encuentra en Ámsterdam desde 2019, cuando entró en vigor el Brexit[17]. En una breve nota, la Agencia rechazó compartir „detalles adicionales mientras la investigación esté en curso" y no informó de si este incidente había afectado o no a la revisión (en marcha desde una semana atrás) de las autorizaciones de comercialización condicional de las vacunas de la Covid-19 desarrollados por las farmacéuticas Pfizer/ BioN ech y Moderna.

La directora de la EMA, Emer Cooke, se dirigió el jueves 17 de diciembre de 2020 al Parlamento Europeo en Bruselas, para responder a las preguntas de los eurodiputados sobre el proceso de revisión de las licencias de uso de las vacunas más avanzadas, pues se esperaba diese su respaldo (como a la postre ocurriera) a la de Pfizer/BioN ech antes del 29 de diciembre de 2020 y a la de Moderna sobre el 12 de enero de 2021[18].

17. Un ataque informático general, que afectó a todas sus oficinas del territorio nacional, obligó al Servicio Público Estatal de Empleo (SEPE, el antiguo INEM) a suspender su actividad en toda España y aplazar todas las citas del día.

Según confirmaron fuentes del SEPE, el virus que afectó a su sistema fue de la familia *ransomware*.

Los ordenadores de la plantilla fueron apagados desde primera hora de la mañana, en que se detectó el ciberataque, como medida de seguridad.

[15] G.sands, "Los senadores presentan un proyecto de ley cibernética para exigir la presentación de informes sobre ataques tipo *ransomware* y ataques a la infraestructura crítica", 29 de septiembre de 2021, pp. 1-7, pp. 2-4 (https://www.cnnespanol.cnn.com).

[16] A.Garrote, "Los bancos y las energéticas, las nuevas víctimas de los ciberdelincuentes", *La Razón*, sábado 5 de marzo de 2022 (https://www.larazon.es)

[17] La Agencia Europea del Medicamento tuvo su sede en Londres hasta 2019, pero cuando el Reino Unido confirmó su decisión de abandonar la Unión Europea, la Agencia trasladó su oficina central a Ámsterdam, desde donde representa a las autoridades nacionales de medicina de los Estados miembros e informa directamente a la Comisión Europea.

[18] P.Dejong, "La Agencia Europea del Medicamento sufre un ciberataque, a punto de aprobar la vacuna de la COVID-19", 10 de diciembre de 2020 (https://es.euronews.com)

El sindicato de empleados públicos Confederación Sindical Independiente de Funcionarios (CSIF) informó de que el virus había paralizado la actividad de las 710 oficinas del SEPE que prestan servicio presencial y de las 52 que lo hace telemáticamente. Y añadió:

> "Los responsables informáticos del SEPE están intentando identificar por dónde ha entrado este virus (*ransomware*), que afectó tanto a los ordenadores de los puestos de trabajo como a los portátiles de la plantilla que se encontraba teletrabajando, con el fin de restablecer los servicios lo antes posible [19].

18. En Suecia, por lo demás, y como consecuencia de ciberataques contra empresas de Estados Unidos, alrededor de 500 supermercados Coop pudieron comprobar cómo, por ejemplo, las cajas registradoras y de autoservicio dejaron de funcionar[20]. El ciberataque se habría perpetrado contra el *software* Kaseya. Los piratas informáticos reclamarían entre 50.000 y 5 millones de dólares según el volumen de la empresa. Coop no utiliza Kesaya directamente en sus sistemas, sino que lo hace uno de sus proveedores de *software*.

Los ciberinvestigadores afirmaron que unas 200 empresas se vieron afectadas por este "colosal" ataque de *ransomware*, que principalmente se dio en Estados Unidos. La empresa informática Kaseya con sede en Florida, cree que la banda de *ransomware* REvil, vinculada a Rusia, fue la responsable.

La Oficina Federal de Investigación (FBI) ya había acusado a esta banda de un hackeo en mayo, ciberataque, éste, que paralizó las operaciones de JBS, el mayor proveedor de carne del mundo[21]

19. Los Gobiernos de los Estados miembros de la Unión Europea registraron en 2020 nada menos que 198 ciberataques contra instituciones públicas, convirtiendo al sector público en el más afectado por las ciberamenazas, según recoge el informe publicado sobre la aplicación de la Estrategia de Seguridad de la Unión Europea.

El estudio señala que la frecuencia y el nivel de sofisticaci n de los ciberataques ha aumentado y tiene como objetivo infraestructuras sensibles para la Unión, como administraciones públicas sanitarias durante la emergencia del coronavirus, además de empresas del sector privado.

Sólo desde el mes de julio (2021), la Unión Europea ha registrado ataques a gran escala contra empresas e instituciones en, al menos, 6 de sus Estados miembro. Los principales afectaron a una cadena de supermercados en Suecia, bases de datos del Gobierno de Estonia, o la Oficina Federal de Estadística de Alemania.

Además, en plena crisis por el coronavirus, los *hackers* atacaron el sistema administrativo de la región de Lazio en Italia, que paralizó la cita de vacunación unos días, o la web para obtener el certificado de vacunación en Países Bajos. Otro ataque de tipo *ransomware* obligó a un hospital en Bélgica a cancelar todas las consultas programadas.

En este contexto, la Unión Europea ha llevado la cuestión de la seguridad en el entorno digital a foros como el G7 y G20 y, en el marco del diálogo bilateral con Estados Unidos, se ha creado un grupo dedicado a la seguridad y competitividad tecnológica[22].

20. El Comité Internacional de la Cruz Roja (CICR) denunció, en enero de 2022, la violación de los datos personales e información confidencial de 515.000 personas, altamente vulnerables, en varios países. Los datos proceden de sesenta sociedades nacionales de la Cruz Roja y de la Luna Roja, que opera en los países de confesión musulmana.

---

[19] A.Sierra/ A.Olcese, "Un ataque informático obliga al SEPE a suspender su actividad en toda España", publicado el 9 de marzo de 2021 (https://www.voxpopuli.com)

[20] J.C.De Santos Pascual, "Cientos de supermercados paralizados en Suecia por el ataque informático a Kaseya en EEUU", 4 de julio de 2021 (https://es.euronews.com)

[21] JBS S.A., empresa de alimentación brasileña, es actualmente el mayor frigorífico de Latinoamérica. Se fundó en 1953, opera en casi 150 países y emplea a más de 125.000 personas. Con 6 décadas de historia, la JBS es actualmente la mayor productora de proteínas del mundo.

[22] EUROPA PRESS, "Los Gobiernos de la UE detectaron 198 ciberataques contra administraciones públicas el año pasado", 8 de diciembre de 2021 (http://www.europapress.com)

Uno de los paquetes de información pirateada es el denominado "Restaurando los lazos familiares", que busca reunir a miembros de una misma familia separados por guerras, migración y desastres.

Debido al ciberataque, el Comité Internacional de la Cruz Roja se vió obligado a "apagar" los sistemas informáticos y dejar de operar este programa de ayuda [23].

21. La Unión Europea se ha mostrado particularmente sensible al uso de la informática contra los hospitales. Tan es así que la Comisión contratará, a lo largo de este año y hasta 2023, 121 profesionales para combatir la ola de ciberataques que se ha extendido durante la pandemia, y que ha tenido entre sus objetivos a hospitales de todo el mundo

Así lo ha hecho saber la Comisión Europea en su respuesta a una pregunta de la eurodiputada española Maite Pagazaurtundúa, del partido Renovar Europa. En la misma, se interrogaba a la Unión sobre las medidas que estaba tomando para repeler ciberataques como el sufrido, en España, por el Servicio Público Estatal de Empleo (*supra* párrafo 17):

> Vemos la multiplicación de ataques cibernéticos al sector de la salud: cibercriminales y servicios de inteligencia de medio mundo dirigen la mayor parte de sus operaciones de secuestro virtual (*ransomware*) y desinformación contra el sector de la salud, concretamente lugares estratégicos en la lucha contra la COVID-19, atacando desde instituciones como la Agencia Europea de Medicamentos hasta laboratorios como el de Moderna u hospitales para pedir rescate ¿Qué planes tiene la Comisión Europea para mejorar las capacidades de la Agencia de la Unión Europea para la Ciberseguridad, que cuenta con solo sesenta y cinco trabajadores? (cuestionó la eurodiputada española).

La respuesta corrió a cargo del comisario francés Thierry Breton:

> La Comisión sabe que los ciberataques han aumentado tanto en términos de número como de complejidad. La pandemia de COVID-19 ha dado lugar a un incremento sin precedentes del teletrabajo y de los servicios ofrecidos en línea. La pandemia ha servido a menudo para facilitar ataques, algo que, en momentos difíciles como estos, puede suponer una especial presión sobre nuestros sistemas sanitarios.

El político francés explicó qué se haría para combatir los ciberataques:

> "A este respecto, la Comisión cree urgente revisar la Directiva sobre la seguridad de las redes y sistemas de información (…) en consonancia con su reciente propuesta, dentro de su planteamiento global reforzado sobre ciberseguridad presentado en el paquete de medidas sobre ciberseguridad el 16 de diciembre de 2020. Si se adopta, la propuesta de la Comisión reforzará los requisitos de seguridad con una lista de medidas específicas y racionalizará los procesos, el contenido y el calendario de la notificación de incidentes".

Breton concluyó así:

> "ENISA, la Agencia de la Unión Europea para la Ciberseguridad, está contratando, para cubrir los puestos ya previstos en el Reglamento de Ciberseguridad, un total de 121 personas (79 agentes temporales, 30 agentes contractuales y 12 expertos nacionales en comisión de servicio) de aquí a 2023. Además, la propuesta de la Comisión de revisión de la Directiva SRI prevé tareas y recursos para cinco equivalentes a tiempo completo adicionales".

En 2020, coincidiendo con los primeros meses de la pandemia, INTERPOL detectó un considerable incremento de los ciberataques. Los cibercriminales aprovecharon el despliegue de infraestructuras de telecomunicaciones por parte de las empresas para el trabajo a distancia. De enero a abril de ese año, uno de los socios de INTERPOL, del sector privado, detectó 907.000 correos basura, 737 incidentes de tipo *malware*, y 48 000 URL maliciosas, todos ellos relacionados con la pandemia[24]

[23] F.Coffrini, "Ciberataque de envergadura contra el Comité Internacional de la Cruz Roja", 25 de enero de 2022 (http://es.euronews.com).

[24] M.Sierra, "La Unión Europea contratará un 'escuadrón' para combatir los ciberataques a hospitales", 8 de febrero de 2022 (https://www.voxpopuli.com)

II. La importancia de proteger "las infraestructuras críticas"

22. Hoy en día, una de las fortalezas de la sociedades de Occidente constituye, simultáneamente, su debilidad, en la medida en que este tipo de sociedades, desarrolladas y altamente tecnificadas, dependen de una serie de servicios esenciales, sin los que no podrían subsistir; como el sistema de transportes, el agua, la electricidad, las telecomunicaciones (…). Por este motivo, hace unos años se acuñó el término *infraestructura crítica* para referirse a la prestación de estos servicios básicos imprescindibles, y, consecuentemente, a la necesidad de su especial protección.

A partir del 11 de septiembre de 2001, cambió el escenario de la seguridad mundial. Se configuró un panorama en el que la destrucción o alteración de ciertos objetivos podrían afectar a la vida y el bienestar tanto de los ciudadanos como de los Estados.

A) En el caso de los Estados Unidos, y tras el 11-S (2001), se reaccionó con la creación del Departamento de Seguridad Interior y una nueva y amplia regulación de esta materia.
B) A nivel europeo, la iniciativa surgió a raíz del 11-M (2004). Tras instar el Consejo Europeo a la Comisión a elaborar una estrategia global sobre protección de las infraestructuras críticas, ésta adoptó una comunicación sobre protección de las mismas en la lucha contra el terrorismo, con propuestas para mejorar la prevención y respuesta de la Unión frente a los atentados terroristas.

Posteriormente, se elaboró una Directiva sobre la identific ción y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección (Directiva 2008/114/CE[25], que entró en vigor el 12 de enero de 2009). La Directiva establece, entre otras cosas, que la responsabilidad principal y última de proteger las infraestructuras críticas corresponde a los Estados miembros y a los operadores de las mismas, e insta a los Estados que integran la Unión a trasponer las disposiciones de la Directiva en los respectivos Derechos internos.

C) España, debido al terrorismo interior, se adelantó, de algún modo, a la Unión en la materia. Así, contamos (lo veremos enseguida) con una normativa, con rango de ley, que delimita las responsabilidades y obligaciones de los diferentes agentes implicados en la protección de las infraestructuras críticas a nivel nacional[26].

23. La protección de las infraestructuras críticas, dada su importancia y las consecuencias que un ciberataque contra ellas puede desencadenar, resulta vital en todo Estado moderno, exigiendo nuevas tecnologías y aún nuevas formas de pensar[27]. Y ello me lleva a reflexiones como las que siguen

La pandemia ha puesto de relieve la importancia de crear una fuerza de trabajo capaz de gestionar el estallido de una crisis en las infraestructuras críticas. Tras un importante ataque cibernético, los países tendrán que depender de fuerza laboral capacitada en materia de seguridad cibernética, para mitigarla, mantener niveles de ciber resiliencia aceptables y garantizar el bienestar de la población.

El sector de las infraestructuras críticas tiende a ser interdependiente. Un ataque o interrupción de una de ellas puede generar una caída en cascada y perturbar con rapidez los elementos centrales de un país. Por eso es conveniente establecer una defensa en capas, de un lado, y, del otro, segmentar la red. Me explico:

— La defensa en capas consiste, precisamente, en crear sistemas de protección en capas; es decir, la nube, los dispositivos tecnológicos de la empresa, los *firewalls* y los correos elec-

[25] *Diario Oficial de la Unión Europea* L 345, 23 de diciembre de 2008, pp, 75-82.

[26] M.J. Caro Bejarano, "La protección de las infraestructuras críticas", Instituto Español de Estudios Estratégicos, *Documento de Análisis*, 021/2011, 27 de julio de 2011, pp. 1-7, pp. 2-3.

[27] M.Alderton, "Contra los ciberataques a infraestructuras críticas, nuevas tecnologías", 7 de diciembre de 2021 (https://redshift.autodesk.es)

trónicos corporativos se protegen por separado. De este modo, se robustece el sistema de seguridad de la organización en su conjunto.

— Segmentar el funcionamiento de la red, particularmente las relacionadas con las de las tecnologías de la información y las tecnologías de operaciones, resulta crucial para no ser víctima de un ciberataque. Para ello, es importante dotarse con sensores de red dentro de los sistemas informáticos internos, pues estos son los encargados de detectar movimientos sospechosos que puedan generar riesgos. Se evita, de este modo, que el sistema de seguridad de una empresa se vea afectado en su conjunto al sufrir un ataque[28].

III. La búsqueda internacional de respuestas normativas a esta realidad

1. Estados Unidos de America

A) Orden ejecutiva del presidente Biden

24. El presidente de los Estados Unidos, Joe Biden, firmó el miércoles 9 de febrero de 2022 una orden ejecutiva para mejorar la ciberseguridad del país[29], tras el ataque informático perpetrado contra el oleoducto *Colonial* (*supra* párrafo 11).

La Orden se propone servir de ejemplo para que el sector privado tome la iniciativa en el fortalecimiento de la ciberseguridad, según declaró un alto funcionario del gobierno en una rueda de prensa en La Casa Blanca[30].

25. La orden ejecutiva establece estándares de ciberseguridad de referencia para todo *software* que adquiera el gobierno, así como que todo *software* utilizado por el mismo cumpla con estos estándares en un plazo de 9 meses desde la fecha de adopción de la Orden[31].

Por otro lado, el texto firmado por el presidente dispone un sistema de respuesta y detección de terminales en todo el gobierno, para ayudar a las agencias federales a compartir información sobre las amenazas cibernéticas[32].

Igualmente, incluye la adopción de un "manual de estrategias" estandarizado y conforme al cual las agencias deben responder inmediatamente a los incidentes cibernéticos que se den en el futuro[33].

Y crea una Junta de Revisión de Seguridad Cibernética (*Cyber Safety Review Board*), integrada por los Departamentos de Seguridad y de Justicia, el Pentágono y, también, el sector privado[34].

26. La orden ejecutiva del presidente Biden marca, pues, el inicio de un proceso de modernización de la defensa cibernética de los Estados Unidos.

Y, seguramente, también el reflejo de un cambio fundamental en mentalidad de las autoridades de este país en relación con las respuestas que las actividades cibernéticas maliciosas merecen[35].

---

[28] *Vid*. G.G. Gómez Morales, "La importancia de la seguridad en las infraestructuras críticas nacionales", 27 de mayo de 2021 (https://www.esan.edu.pe)

[29] *Executive Order on Improving the Nation's Cybersecurity.* May 12, 2021, Presidential Actions, https://www.whitehouse.gov/briefing-roo , pp. 1-18.

[30] SANTIAGO, Michael M., "El oleoducto Colonial, el más importante del país, reanuda su actividad", Madrid, 13 de febrero de 2022, https://www.europapress.es, pp. 1-3, p. 1.

[31] *Executive Order on Improving the Nation's Cybersecurity, op. cit.* (nota 29), Secciones 1 y 9, pp. 1 y 16.

[32] *Ibidem,* Secciones 2, 7 y 8, pp. 2-4, 13-15, 15-16.

[33] *Ibidem,* Sección 6, pp. 12-13.

[34] *Ibidem*, Sección 5, pp. 11-12.

[35] *Ibidem*, Secciones 3 y 4, pp. 4-6 y 6-10.

B) Proyectos de Ley

27. El Comité de Seguridad Nacional de la Cámara de Representantes de Estados Unidos aprobó, el lunes 17 de mayo de 2021, 5 proyectos de ley bipartidistas para reforzar las capacidades de defensa contra los ciberataques dirigidos contra organizaciones e infraestructuras críticas estadounidenses:

— Proyecto de ley de mitigación de la vulnerabilidad de la ciberseguridad[36]
— Proyecto de ley de mejora de la seguridad cibernética estatal y local[37].
— Proyecto de ley de ejercicio cibernético de la Agencia de Ciberseguridad y
— Seguridad de las Infraestructuras (CISA)[38].
— Proyecto de ley de seguridad de oleoductos[39].
— Proyecto de ley de dominios críticos para la seguridad nacional[40].

Estos proyectos de ley se presentaron como resultado directo de la supervisión efectuada por el Comité de Seguridad Nacional de los ciberataques sufridos por empresas y entidades de los Estados Unidos en los últimos dos años, incluido el ya mencionado *ransomware* que obligó a *Colonial Pipeline* a cerrar el mayor oleoducto del país; aunque *Colonial* pagó un rescate de 5 millones de dólares, ello no impidió una escasez de combustible a gran escala que afectó a varios Estados del noreste (*vid. supra* párrafos 10-14).

Además de la normativa para mejorar la seguridad de los oleoductos y gasoductos de Estados Unidos, los proyectos de ley también autorizan a la Agencia de Ciberseguridad y Seguridad de las Infraestructuras (CISA) para, entre otros cometidos, promover la realización de pruebas periódicas de preparación para los ciberataques[41].

28. Más aún. Los principales senadores de la Comisión de Seguridad Nacional presentaron un proyecto de ley el martes 28 de septiembre de 2021, para exigir a las empresas de infraestructura crítica que informen al gobierno federal de todo ataque cibernético que sufran. La iniciativa exige que la mayoría de las organizaciones informen, en concreto, al gobierno si realizan pagos por ataques de *ransomware*.

Si el proyecto de ley se promulga creará el primer requisito nacional para que los dirigentes de infraestructura crítica informen cuando sus sistemas hayan sido violados.

Asimismo, el senador Chuck Schumer, líder de la mayoría demócrata en el Senado, solicitó que el presupuesto de la Agencia de Ciberseguridad e Infraestructura (CISA), del Departamento de Seguridad Nacional, se incrementase en 500 millones de dólares[42].

Con este proyecto de ley, CISA tendrá más autoridad. Para ser precisos, la Agencia podrá citar a las entidades que no informen sobre ciberataques o pagos por *ransomware.* Y de no acatar la citación, se les podría prohibir llevar a cabo contrataciones con el gobierno federal.

No cabe duda que los esfuerzos que la actual Administración Demócrata y otros órganos estatales están haciendo en esta cuestión son muy importantes[43].

---

[36] 117 Congress, 1 th. session , HR 2980, g:\VHLC\040721.051.xml (798662/1), april 7, 2021(1:04 p.m.), pp. 1-5.

[37] 117 Congress, 1 th. session , HR 3138, g:\VHLC\050621.133.xml (799137/5), may 6, 2021 (4:24 p.m.), pp. 1-39.

[38] 117 Congress, 1 th. session , HR 3223, g:\VHLC\051221.138.xml (801878/2), may 12, 2021 (3:43 p.m.), pp. 1-6.

[39] 117 Congress, 1 th. session , HR 3243, g:\VHLC\051121.218.xml (802006/6), may 11, 2021 (7:53 p.m.), pp. 1-7.

[40] 117 Congress, 1 th. session , HR 3264, g:\VHLC\051321.236.xml (798260/8), may 13, 2021 (6:32 p.m.), pp. 1-7.

[41] Bleeping Computer, "Estados Unidos presenta proyectos de ley para proteger las infraestructuras críticas de los ciberataques", 22 de mayo de 2021 (https://www.ciberseguridadlatam.com)

[42] SANDS, Geneva, "Los senadores presentan un proyecto de ley…", *op. cit.* (nota 15 *supra*), pp. 2-4; VALADES, Bernardo, "Estados Unidos y Europa contemplan nuevas leyes para enfrentar las seis de la amenazas", 14 de junio de 2021, pp. 1-3 [SEGURILATAM. Revista de Seguridad Integral, archivado en: ActualidadCiberseguridadIfraestructurasCriticaSaludSeguridadporsectoresTecnologiasyserviciosTransporte])

[43] C.Sánchez, "Estados Unidos presenta un nuevo proyecto de ley ciber", 4 de octubre de 2021, pp. 1-6, pp. 1-2 [https://cybersecuritynews.es])

29. Finalmente, el Senado de Estados Unidos aprobó el martes 1 marzo de 2022, por unanimidad, un proyecto de ley bipartidista que está destinado a fortalecer la ciberseguridad dentro de sus fronteras. Esta nueva legislación fue originalmente presentada en el Senado el 8 de febrero de 2022[44], siendo sus promotores Gary Peters (senador demócrata del Estado de Michigan y presidente del Comité de Asuntos Gubernamentales y Seguridad Nacional) y Rob Portman (senador republicano del Estado de Ohio y miembro de alto rango del mismo Comité).

La ley, de más de 200 páginas, combina partes de tres proyectos de ley diferentes que los propios Peters y Portman presentaron ante el Comité: la Ley de Informes de Incidentes Cibernéticos (CIRA), la Ley Federal de Modernización de la Seguridad de la Información de 2021 (FISMA) y la Ley Federal de Empleos y Mejora de la Nube Segura (FSCIJA)[45].

El proyecto de ley aprobado por el Senado estadounidense incluye varias medidas orientadas a reforzar la ciberseguridad tanto en el sector público como en el privado, y a modernizar la postura de ciberseguridad del gobierno. Para ello, incluye disposiciones como:

— Exigir a los propietarios y operadores de infraestructura crítica y a las agencias federales civiles que informen de los ciberataques a la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) en un margen máximo de 72 horas, y de los pagos de *ransomware* en un margen de solo 24 horas.
— Otra novedad significativa de la nueva ley es que autoriza durante cinco años el Programa Federal de Gestión de Riesgos y Autorizaciones (FedRAMP) para garantizar que las agencias federales puedan "adoptar de forma rápida y segura tecnologías basadas en la nube que mejoren las operaciones y la eficiencia del gobierno"

Su aprobación en el Senado se produce en un contexto de repetidas advertencias por CISA y otras agencias del gobierno de los Estados Unidos sobre el potencial incremento de ciberataques rusos por la escalada del conflicto en Ucrania[46], una amenaza por la que tanto Peters como Portman consideran que su legislación se necesita "con urgencia".

Tras recabar el apoyo unánime del Senado, la legislación debe ser aprobada por la Cámara y ser firmada por el presidente Joe Biden para convertirse oficialmente en ley. De ser así, también actualizaría las leyes de ciberseguridad estadounidenses para mejorar la coordinación entre las agencias y requeriría que el gobierno adopte un enfoque de ciberseguridad basado en el riesgo.

2. La Unión Europea

30. Las actividades informáticas maliciosas aumentan también en toda Europa, siendo cada vez más sofisticadas. Es conveniente, por ello, una respuesta más firme en materia de seguridad; solo así podrá operarse en un ciberespacio que generará entre los ciudadanos una mayor confianza en la digitalización[47]

La creciente relevancia de las amenazas que provienen del ciberespacio se hizo patente en febrero de 2013, cuando la Comisión Europea y la Alta Representante de la Unión Europea para Asuntos Exteriores y Política de Seguridad presentaron conjuntamente la Estrategia de Ciberseguridad de la Unión Europea: un ciberespacio abierto protegido y seguro.

[44] S.Montes, "El Senado de EE.UU. aprueba por unanimidad una importante legislación de ciberseguridad **(**El consenso se produce en medio de las constantes alertas sobre el creciente riesgo de ciberataques por parte de Rusia por la escalada del conflicto en Ucrania)", 4 de marzo de 2022 https://www.escudodigital.com).

[45] 117TH CONGRESS 2D SESSION. S.3600. An Act to improve the cybersecurity of the Federal Government, and for other purposes. This Act may be cited as the ''Strengthening American Cybersecurity Act of 2022''), pp. 1-212.

[46] *Vid*. E.Cubeiro Cabello, "El ciberespacio en la guerra de Ucrania", *op. cit*. (nota 4 *supra*), pp. 1-14.

[47] Sobre la creciente profundización e intensidad del interés de la Unión Europea en la ciberseguridad y en responder con una firme defensa a los ciberataques, *vid*. PIERNAS LÓPEZ, J.J., "La respuesta de la Unión Europea a las amenazas del ciberespacio", en CERVELL HORTAL, M.J. (Directora), *Nuevas tecnologías en el uso de la fuerza: drones, armas autónomas y ciberespacio*, Thomson Reuters/Aranzadi, Cizur Menor (Navarra), 2020, pp. 279-308; ID., *Ciberdiplomacia y ciberdefensa en la Unión Europea* Thomson Reuters/Aranzadi, Cizur Menor (Navarra), 2020, pp. 57 ss, 89 ss., 143 ss.

La Unión aumentó notablemente su ambición en materia de ciberseguridad con la adopción, el 13 de septiembre de 2017, del conocido como el conjunto de medidas de ciber seguridad o *EU Cyber Security Package*. Este incluía, entre otras, una propuesta de creación de la Agencia Europea de Ciberseguridad, basada en la existente Agencia de Seguridad de la Redes y de la Información de la Unión Europea, de un Centro Europeo de Investigación y con Competencias en materia de Ciber seguridad, la inclusión de la libertad de ciberdefensa en el Marco de la cooperación estructurada permanente y el fondo europeo de defensa, y la elaboración de un régimen de certificación europe [48].

En diciembre de 2020, la Comisión Europea y el Servicio Europeo de Acción Exterior (SEAE) presentaron una nueva Estrategia de Ciberseguridad de la Unión Europea[49]. Su objetivo: reforzar la resiliencia de la Unión antes la ciberamenazas y garantizar que todos los ciudadanos y empresas puedan beneficiarse plenamente de servicios digitales seguros y fiable [50]. La nueva estrategia sugiere propuestas concretas para la adopción de instrumentos normativos (tanto de actuación como de inversión).

El 22 de marzo de 2021, el Consejo adoptó unas Conclusiones sobre la Estrategia de Ciberseguridad. En ellas, los ministros de la Unión Europea decidieron, como objetivo esencial, la consecución de una autonomía estratégica preservando a la vez una economía abierta, para lo que resultaba necesario aumentar la capacidad de adoptar decisiones autónomas en el ámbito de la ciberseguridad.

La Unión Europea está trabajando, asimismo, en dos propuestas legislativas para abordar los riesgos actuales y futuros *en* y *fuera de* Internet:

— Una Directiva actualizada para proteger mejor las redes y los sistemas de información.
— Y una nueva Directiva sobre la resiliencia de las entidades críticas.

La Unión cuenta, en fin, como ya he apuntado *supra*, con una nueva Agencia para la Ciberseguridad, con un papel reforzado y un mandato permanente. Ha mantenido el mismo acrónimo, ENISA (https://www.enisa.europa.eu/). Esta agencia proporciona apoyo a los Estados miembros, las instituciones de la Unión y otras partes interesadas para hacer frente a los ciberataques.

31. La Directiva sobre la Seguridad de la Redes y Sistemas de Información, adoptada en 2016 (conocida como Directiva NIS), fue la primera medida legislativa a escala de la Unión destinada a estrechar la cooperación entre los Estados miembros en lo relativo a la ciberseguridad. En ella se establecieron obligaciones de seguridad para los operadores de servicios esenciales (en sectores vitales como la energía, el transporte, la sanidad y las finanzas) y los proveedores de servicios digitales (mercados en línea, motores de búsqueda y servicios en la nube)[51].

En diciembre de 2020, la Comisión Europea propuso una revisión de la Directiva NIS (NIS-2) para sustituir a la de 2016[52]. La nueva propuesta responde a la evolución de las amenazas y tiene en cuenta la transformación digital que se ha visto acelerada por la crisis de la COVID-19:

---

[48] J.J.Piernas López, "La respuesta de la Unión Europea a las amenazas del ciberespacio", *op. cit.* (nota 47), pp. 283-284, 287-288; ID., *Ciberdiplomacia y ciberdefensa en la Unión Europea, op. cit.* (nota 47), pp. 38-51.

[49] EUROPEAN COMMISSION/HIGH REPRESENTATIVE OF THE UNION FOR FOREIGN AFFAIRS AND SECURITY POLICITY*, Joint Communication to the European Parliement and the Councuil. The EU'Cybersecurity Strategy for the Digital Decade*, Burselas, 16 de diciembre de 2020, JOIN (2020) 18 final, pp. 1-28

[50] COMISIÓN EUROPEA (comunicado de prensa), "Nueva Estrategia de Ciberseguridad de la UE y nuevas normas para aumentar la resiliencia de las entidades críticas físicas y digitales", IP/020/2391, Bruselas, 16 de diciembre de 2020, pp. 1-5. La nueva Estrategia de la Unión en este ámbito ha sido valorada con escaso entusiasmo, digámoslo así, por algunos comentaristas: véase, por ejemplo, KASPER, A. y VERNYGORA, V., "The EU's cybersecurity: a strategic narrative of a cyber power or a confusing policy for a local common market", *Cuadernos Europeos de Deusto*, núm. 65/2021, pp. 29-71.

[51] Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, *Diario Oficial de la Unión Europea*, L 194, 19 de julio de 2016, pp. 1 ss.

[52] COMISIÓN EUROPEA, Propuesta para una Directiva del Parlamento Europeo y del Consejo sobre medidas para un alto nivel común de ciberseguridad en toda la Unión, por la que se deroga la Directiva (UE) 2016/1148 (Texto pertinente a efectos del EEE), Bruselas, 16.12.2020, COM(2020) 823 final, 2020/0359 (COD) (SEC(2020) 430 final} - {SWD(2020) 344 final} - {SWD(2020) 345 final

— Con este fin, la propuesta de la Comisión amplía el alcance de la actual Directiva NIS, agregando nuevos sectores en función de su importancia para la economía y la sociedad e introduciendo un límite de tamaño claro, lo que significa que se incluirán en la misma todas las medianas y grandes empresas en sectores seleccionados.
Al mismo tiempo, deja cierta flexibilidad para que los Estados miembros identifiquen entidades más pequeñas con un alto perfil de riesgo de seguridad
— La propuesta también elimina la distinción entre operadores de servicios esenciales y proveedores de servicios digitales.
Las entidades se clasifica ían en función de su importancia, y se dividirían, respectivamente, en categorías esenciales e importantes con la consecuencia de estar sujetas a diferentes regímenes de supervisión.
— La propuesta refuerza los requisitos de seguridad para las empresas, al imponer un enfoque de gestión de riesgos que proporciona una lista mínima de elementos básicos de seguridad que deben aplicarse; e introduce, asimismo, disposiciones más precisas sobre el proceso de notificación de incidentes, el contenido de los informes y los plazos
— Además, la Comisión propone abordar la seguridad de las cadenas de suministro y las relaciones con los proveedores exigiendo a las empresas individuales que aborden los riesgos de ciberseguridad en esta cuestión.
A nivel europeo, la propuesta refuerza la ciberseguridad de la cadena de suministro para tecnologías clave de la información y la comunicación. Los Estados miembros, en cooperación con la Comisión y ENISA, llevarán a cabo evaluaciones de riesgo coordinadas de las cadenas de suministro críticas, basándose en el enfoque adoptado con éxito en el contexto de la Recomendación de la Comisión sobre ciberseguridad de las redes 5G[53].
— La propuesta introduce medidas de supervisión y requisitos de ejecución más rigurosos para las autoridades nacionales, propiciando la armonización de los regímenes sancionadores en todos los Estados miembros.
— La propuesta de la Comisión establece un marco básico con actores clave responsables de la divulgación coordinada de vulnerabilidades recientemente descubiertas en toda la Unión Europea, así como la creación de un registro de la Unión en el que opera la Agencia de Ciberseguridad de la Unión Europea (ENISA).

El Consejo, en fin y por acabar, llegó a una Orientación general sobre la nueva directiva en diciembre de 2021[54].

La tramitación del proyecto de Directiva sigue avanzando[55], con la aprobación por el Comité de Industria del Parlamento Europeo de las enmiendas presentadas. La norma proyectada se centra en la necesidad de reforzar la importancia de esta regulación como principal legislación horizontal en el ámbito de la ciberseguridad y tiene como objetivo garantizar que la futura legislación sectorial no modifique sus principios fundamentales. Las principales novedades introducidas con esta nueva versión del proyecto de Directiva NIS 2 serían, en síntesis, las siguientes:

— La ampliación del ámbito de aplicación de la nueva Directiva NIS 2, mediante dos técnicas:

[53] RECOMENDACIÓN (UE) 2019/534 DE LA COMISIÓN de 26 de marzo de 2019 Ciberseguridad de las redes 5G, *Diario Oficial de la Unión Europea*, L 88, 29 de marzo de 2019, pp. 42-47.

[54] CONSEJO EUROPEO. CONSEJO DE LA UNIÓN EUROPEA, "Ciberseguridad: cómo combatir la Unión Europea las amenazas cibernéticas", pp. 1-11, pp. 1-7 (https://www.consilium.europa.eu, 9 febrero 2022).

[55] Parlamento Europeo 2019-2024 Documento de sesión 4.11.2021, INFORME A9-0313/2021 sobre la propuesta de Directiva del Parlamento Europeo y del Consejo relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad y por la que se deroga la Directiva (UE) 2016/1148 (COM(2020)0823 – C9-0422/2020 – 2020/0359(COD)) Comisión de Industria, Investigación y Energía Ponente: Bart Groothuis Ponente de opinión (*): Lukas Mandl, Comisión de Libertades Civiles, Justicia y Asuntos de Interior (*) ES Comisión asociada – artículo 57 del Reglamento interno Unida en la diversidad PE692.602v02-00 ES RR\1242692ES.docxPR_COD_1amCom

- La ampliación del concepto entidades esenciales, al incluirse en él sectores o actores no previstos en la anterior Directiva NIS, como por ejemplo energía, transportes, banca, infraestructuras de los mercados financieros, sanidad, agua potable, aguas residuales, infraestructura digital, administración pública y sector espacial.
- Y la introducción de un nuevo concepto denominado entidades de "sectores importantes". En la exposición de motivos del texto publicado se avanza que estos sectores incluirán, entre otros: servicios postales y de mensajería, gestión de residuos, fabricación, producción y distribución de sustancias y mezclas químicas, producción, transformación y distribución de alimentos, fabricación y proveedores de servicios digitales.

A pesar de lo anterior, cabe destacar que la normativa nacional de desarrollo de la actual Directiva NIS[56], ya prevé su aplicación a la mayoría de las entidades a las que el borrador de Directiva NIS 2 extiende su ámbito de aplicación, por lo que esta modificación tendrá una limitada incidencia a nivel nacional.

— Se destaca la importancia de armonizar la normativa que regula la prevención, detección y respuesta a las ciberamenazas y ciberataques. Para ello, se impone a la Agencia de la Unión Europea para la Ciberseguridad (ENISA) la responsabilidad de proveer a los Estados miembros y las autoridades competentes la orientación para que adapten sus estrategias nacionales de ciberseguridad en vigor a los requisitos y obligaciones establecidos en la Directiva.
— En lo relativo a los nuevos requisitos de seguridad exigidos se incluyen, entre otros, la respuesta a incidentes, la seguridad de la cadena de suministro, el cifrado y la divulgación de vulnerabilidades.
— En cuanto a las sanciones, seguirán siendo los Estados miembros los encargados de establecer el régimen sancionador aplicable, adoptando todas las medidas necesarias (efectivas, proporcionadas y disuasorias) para su ejecución.

Cabe recordar que, en el caso de España, las sanciones aplicables a las infracciones en materia de ciberseguridad se regulan en el Real Decreto-ley 12/2018, como sanciones leves, graves y muy graves. La cuantía de las sanciones oscila desde una amonestación o multa para las muy leves (no someterse, por ejemplo, a una auditoría de seguridad) hasta 1.000.000 euros para las muy graves (como el incumplimiento reiterado de la obligación de notificar incidentes con efectos perturbadores signific - tivos en el servicio).

Según el Parlamento Europeo la necesidad de esta nueva normativa se fundamenta en la aplicación y desarrollo no armónico que se ha producido por parte de los Estados miembros de la Unión, lo que ha generado niveles insuficientes de ciberseguridad. Dado que el nivel actual de ciber-amenazas muy elevado, actualizar esta legislación era urgente, resultando, pues, indispensables la prevención y el cumplimiento[57].

32. La propuesta de Directiva sobre la resiliencia de las entidades críticas (REC) amplía el ámbito de aplicación y la profundidad de la Directiva sobre infraestructuras críticas europeas de 2008. Se incluyen 10 nuevos sectores:

— Energías.
— Transporte.
— Banca.
— Infraestructura de los mercados financieros

[56] Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información (*BOE* de 8 de septiembre de 2018) y el Real Decreto 43/2021, de 26 de enero (*BOE* de 28 de enero de 2021) que desarrolla el primer Real Decreto-ley.

[57] M.Ferrer/ J.A.Eguiluz, "Unión Europea/Ciberseguridad: nueva versión del proyecto de Directiva NIS 2", 24 de noviembre de 2021 (https://www.cuatrecasas.com)

— Sanidad.
— Agua potable.
— Aguas residuales.
— Infraestructuras digitales.
— La administración pública.
— Y el espacio.

En el marco de la Directiva propuesta, los Estados miembros podrían adoptar una estrategia nacional con el objetivo de reforzar la resiliencia de las entidades críticas y efectuar evaluaciones periódicas sobre el riesgo.

Éstas evaluaciones también ayudarían a identificar un grupo más reducido de entidades críticas que estarían obligadas a mejorar su resiliencia frente a riesgos no cibernéticos, la adopción de medidas técnicas y organizativas o la notificación de incidentes.

Por su parte, la Comisión prestaría apoyo complementario a los Estados miembros y a las entidades críticas, por ejemplo, mediante la aplicación de mejores prácticas y ejercicios para poner a prueba su resiliencia.

33. Como he apuntado, la creciente amenaza que suponen los ciberataques motivó una reacción cada vez más decidida de la Unión Europea, que se vio culminada con la adopción de un Marco jurídico de medidas restrictivas para hacer frente a los mismos compuesto:

— Por la Decisión (PESC) 2019/797 del Consejo, de 17 de mayo de 2019, relativa a medidas restrictivas contra los ciber ataques que amenazan a la unión o a sus estados miembros[58].
— Y el Reglamento (UE) 2019/796 del Consejo, de 17 de mayo de 2019, relativo a medidas restrictivas contra los ciber ataques que amenazan a la Unión o a sus Estados miembros[59].

Más concretamente, el Marco adoptado permite a la Unión, por primera vez, imponer sanciones a personas o entidades responsables de ciberataques o tentativas de ciber ataques; o que presten apoyo financiero, técnico o material para ello; o estén implicadas de algún otro modo, así como a otras personas y entidades asociadas con ellas.

Las medidas restrictivas consisten en:

— La prohibición de entrada a la Unión en el caso de las personas.
— Y la inmovilización de activos en el caso de personas y entidades
— Las primera sanciones por ciberataques se impusieron el 30 de julio de 2020.

34. El ciberespacio se considera ya el quinto ámbito bélico, tan vital para las operaciones militares como la tierra el mar, el aire y el espacio.[60]

La Unión Europea coopera en materia de defensa en el ciberespacio por medio de la Agencia Europea de Defensa (AED), en colaboración con la Agencia de la Unión Europea para la Ciberseguridad y Europol. La AED apoya a los Estados miembros en la creación de unidades de personal militar especializado en ciberdefensa y garantiza la disponibilidad de tecnología de ciberdefensa (tanto proactiva como reactiva).

La Estrategia de Ciberseguridad de la Unión Europea, adoptada en diciembre de 2020 por la Comisión y el Servicio Europeo de Acción Exterior, refuerza:

[58] ST/7299/2019/INIT, *Diario Oficial de la Unión Europea,* L 129I, 17 mayo 2019, pp. 13-19.

[59] ST/7302/2019/INIT, *Diario Oficial de la Unión Europea,* L 129I 17 mayo 2019, pp. 1-12.

[60] REDACCIÓN, "Una guerra mundial ya se libra en el ciberespacio con sofisticados ataques de *ransomware*", 4 de julio de 2021 (https://bajopalabra.com.mx); A.González, "Ciberespacio es el nuevo campo de batalla entre naciones", 14 de octubre de 2021 (https://digitalpolicylaw.com).

— La coordinación en materia de ciberdefensa.
— La cooperación y la creación de capacidades de ciberdefensa.

35. En diciembre de 2020, el Consejo y el Parlamento Europeo alcanzaron un acuerdo informal para crear el Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad respaldado por una red de centros nacionales de coordinación

Cinco meses después, el Parlamento Europeo y el Consejo adoptaron el reglamento 2021/887, de 20 de mayo de 2021, por el que se establecen el Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad y la Red de Centros Nacionales de Coordinación[61]. Sus objetivos son:

— Seguir mejorando la ciber resiliencia.
— Contribuir a la implantación de tecnología de última generación en materia de ciber seguridad.
— Proporcionar apoyo a las empresas emergentes y las pymes del sector de la ciberseguridad.
— Reforzar la investigación y la innovación en materia de ciber ciberseguridad.
— Contribuir a colmar el déficit de capacidades en materia de ciberseguridad

Los Estados miembros de la Unión Europea eligieron Bucarest como sede del nuevo centro[62].

3. Particular referencia a nuestro país, España

36. En el contexto de los ataques con armas cibernéticas, el concepto de *infraestructura crítica* es esencial también *en* y *para* nuestro país. Las infraestructuras críticas son el conjunto de:

> "instalaciones, redes, sistemas y equipos físicos y de tecnología de la información… cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales"[63].

La "criticidad" de una infraestructura se fija en atención a tres criterios:

— El número de víctimas o de lesiones graves que, de ser atacada, puede generar.
— El impacto económico en función de las pérdidas y el deterioro de productos o servicios (incluido el eventual impacto medio ambiental).
— Y el impacto público producido por la alteración de la vida ciudadana.

En España, el anexo a la Ley 8/2011 de Protección de las Infraestructuras Críticas (que, asimismo, se extiende a la protección de las Infraestructuras Críticas Europeas) , y que transpone al Derecho español la Directiva 2008/114/CE, agrupa estas en varios sectores (doce para ser exactos)[64].

Estas infraestructuras dependen de los sistemas de comunicaciones y, por tanto, el riesgo de interrupción por ataques cibernéticos ha aumentado considerablemente. Las infraestructuras críticas

[61] *Diario Oficial de la Unión Europea*, L 202, 8 de junio de 2021, pp. 1-31.

[62] CONSEJO EUROPEO. CONSEJO DE LA UNIÓN EUROPEA, "Ciberseguridad: cómo combatir la Unión Europea las amenazas cibernéticas", pp. 1-11, pp. 8-10 (https://www.consilium.europa.eu, 9 febrero 2022).

[63] Artículo 2, d y e de la Ley 8/2011, de 28 de abril*, por la que se establecen medidas para la protección de las infraestructuras críticas* (*BOE* de 29 de abril de 2011).

[64] Administración (servicios básicos, instalaciones, redes activas de información, principales lugares y monumentos nacionales), Espacio, industria nuclear, industria química, instalaciones de investigación, agua (embalses, almacenamiento, tratamiento y redes), energía (centrales y redes de energía), salud, tecnología de la Información y las Comunicaciones, transporte (aeropuertos, puertos, instalaciones intermodales, ferrocarriles y redes de transporte público, sistemas de control de tráfico), alimentación, sistema Financiero y Tributario (Banca, valores, inversiones).

españolas se detallan en un Catálogo que integra 3.700 infraestructuras, de las que el 80 por 100 corresponden al sector privado. La Ley 8/2011 establece la creación, por el Ministerio del Interior, de un Catálogo Nacional de Infraestructuras Estratégicas:

> "Instrumento que contendrá toda la información y valoración de las infraestructuras estratégicas del país, entre las que se hallarán incluidas aquellas clasificadas como Críticas o Críticas Europeas, en las condiciones que se determinen en el Reglamento que desarrolle la presente Ley" (artículo 4.1).

El Real Decreto 704/2011, de 20 de mayo, aprueba el Reglamento de protección de las Infraestructuras Críticas[65] que regula (Título I, Capítulo II, artículos 3-5), el referido Catálogo. Este viene a ser una base de datos en la que se especifican las medidas de protección ante una eventual amenaza contra dichas Infraestructuras, la "criticidad" y los planes de reacción "que activen una respuesta ágil, oportuna y proporcionada, de acuerdo con el nivel y características de la amenaza de que se trate" (artículo 3.2). El Catálogo, un registro de carácter administrativo, contiene información "completa, actualizada y contrastada" de todas las infraestructuras estratégicas ubicadas en el territorio español, "incluyendo las críticas, así como aquellas clasificadas como críticas europeas que afecten a España, con arreglo a la Directiva 2008/114/CE" (artículo 3.1).

El Catálogo Nacional de Infraestructuras Estratégicas tiene, según la legislación española en materia de secretos oficiales, "la calificación de SECRETO", conferida por Acuerdo del Consejo de Ministros, de 2 de noviembre de 2007 (artículo 4.3).

37. La Estrategia de Seguridad Nacional de 2021, en fin, afirma que los ataques contra las infraestructuras críticas constituyen "riesgos y amenazas a la seguridad nacional", que con la:

> "progresión digitalizada y la adopción de nuevas tecnologías (…) podría aumentar el riesgo de sufrir brechas de seguridad (…) en el control de los sistemas que operan las infraestructuras críticas"[66].

Y la Estrategia de Ciberseguridad de 2019 destaca las "amenazas contra las infraestructuras críticas" como objetivo posible de los grupos terroristas. A tal efecto, en la línea de acción 2 (*garantizar la seguridad y resiliencia de los activos estratégicos para España*), fijada por la Estrategia de Ciberseguridad, nuestro país se propone:

> "asegurar la plena implantación del Esquema Nacional de Seguridad, del Sistema de Protección de las Infraestructuras Críticas, y el cumplimiento y armonización de la normativa sobre protección de infraestructuras críticas y servicios esenciales, con un enfoque prioritario basado en el riesgo (apartado 3)[67].

IV. Las contramedidas, como instrumento de defensa en el plano internacional

1. Algunos supuestos de la práctica

38. Las tradicionales sospechas sobre la injerencia rusa en Estados Unidos se han convertido, finalmente, en acusación formal. La Casa Blanca ha apuntado, por primera vez, al Servicio de Espionaje Exterior ruso (SVR) e impuesto sanciones contra una treintena de individuos y entidades, por ciberataques diversos (que califica de "acciones internacionales desestabilizadoras"). Las sanciones (las más duras des-

[65] *BOE* de 21 de mayo de 2011.

[66] PRESIDENCIA DEL GOBIERNO: *Estrategia de Seguridad Nacional 2021*, Madrid, 2021, pp. 1-114, especialmente pp. 52, 58 (la *Estrategia* se aprobó por Real Decreto 1150/2021, de 28 de diciembre, y se publicó en el *BOE*, de 31 de diciembre de 2021, pp. 167795-167830).

[67] MINISTERIO DE LA PRESIDENCIA, RELACIONES CON LAS CORTES E IGUALDAD: *Estrategia Nacional de Ciberseguridad 2019*, Madrid, junio 2019, pp. 1-68 (por Orden PCI/487/2019, de 26 de abril, se publica tras su aprobación por el Consejo de Seguridad Nacional en el *BOE*, 30 de abril de 2019), BOE 30 de abril, pp. 43444 y 43449-43450.

de la presidencia de Donald Trump) se dirigieron contra la mismísima línea de flotación de la economía rusa. Además, el Departamento del Tesoro emitió otra directiva que prohíbe a las instituciones financiera estadounidenses comprar deuda pública del Banco Central ruso a partir del mes de junio de 2021.

Las sanciones de Estados Unidos afectan a 16 entidades y 16 individuos e incluyen la expulsión de una decena de empleados de la Embajada rusa en Washington, funcionarios de inteligencia incluidos, por "intentos dirigidos por el Gobierno ruso para influir en las elecciones de 2020 y otros actos de desinformación e interferencia". Todos los sancionados vieron congelados sus activos en Estados Unidos.

Al anunciar las sanciones, la Casa Blanca acusó formalmente al Servicio de Espionaje Exterior de Rusia (SVR) de haber perpetrado, en concreto, el ciberataque masivo que penetró los sistemas informáticos de la Administración estadounidense y de grandes compañías mediante un programa de *SolarWinds* (*supra* párrafo 10).

Entre los individuos implicados figura Alexéi Gromov, miembro de la Administración Presidencial rusa (subjefe de personal de la misma), explicó el comunicado del Tesoro.

En el texto que anuncia la imposición de sanciones, hecho público por la Casa Blanca, Washington acusa también a Moscú, en una referencia que parece apuntar directamente a la situación en Ucrania:

> de "socavar la seguridad en países y regiones importantes para la seguridad nacional de Estados Unidos; y violar principios bien establecidos del derecho internacional, incluido el respeto por la integridad territorial de los Estados, [que] constituyen una amenaza inusual y extraordinaria para la seguridad nacional, la política exterior y la economía de Estados Unidos".

Junto con el Reino Unido, Australia, Canadá y la Unión Europea, Washington también sancionó a 8 personas y entidades en la órbita del Kremlin por la ocupación (en 2014) de Crimea. Estados Unidos denunció, en particular, las presuntas violaciones de derechos humanos en un centro de detención de Simferópol, la capital de Crimea.

Un reciente informe no clasificado de los servicios de inteligencia estadounidense asegura que el presidente ruso, Vladimir Putin, autorizó campañas de influencia destinadas a dañar la candidatura del presidente Biden durante las elecciones de 2020 e impulsar la del republicano Donald Trump, según la CBS, que cita un informe difundido por la Oficina del Director de Inteligencia Nacional

Entre "las acciones que ha emprendido el Gobierno ruso contra nuestra soberanía e intereses", indica la Casa Blanca, figura también su propuesta a los talibanes para cometer atentados contra las fuerzas de los Estados Unidos en Afganistán, revelada en 2020 por el *The New York Times*. No obstante, "dado lo delicado del asunto, que compromete la seguridad y el bienestar de nuestros soldados", la investigación discurrirá por canales diplomáticos y de inteligencia.[68]

39. También el Consejo de la Unión Europea decidió imponer, el 30 de julio de 2020, medidas restrictivas contra personas y entidades responsables de diversos ataques informáticos. Se trataba de una respuesta a, entre otros, el intento de ciberataque contra la OPAQ (Organización para la Prohibición de las Armas Químicas). El Alto Representante de la Unión, Sr. Borrell, hizo una declaración pública al respecto en nombre de la Unión:

> "A fin de prevenir, desincentivar e impedir mejor estas conductas maliciosas en el ciberespacio y responder a ellas, el Consejo ha decidido hoy aplicar medidas restrictivas a seis personas y tres entidades u organismos involucrados en ciberataques con efectos importantes o en tentativas de ciberataque con efectos potencialmente importantes que constituyen una amenaza externa para la Unión Europea o sus Estados miembros, o con efectos importantes en terceros Estados u organizaciones internacionales. Las medidas en cuestión son la prohibición de viajar y la inmovilización de bienes de las personas físicas y la inmovilización de bienes de las entidades u organismos. También está prohibido poner fondos a disposición directa o indirecta de las personas y entidades u organismos incluidos en la lista".[69]

[68] M.A.Sánchez-Vallejo, "Biden impone duras sanciones a Moscú por los ciberataques y la injerencia en las elecciones", Nueva York, 15 de abril de 2021 (https://elpais.com)

[69] CONSEJO DE LA UE, "Declaración del alto representante, Josep Borrell, en nombre de la UE: respuesta de la Unión

Este tipo de medidas constituye una de las opciones ofrecidas por los instrumentos de ciberdiplomacia de la Unión para impedir, disuadir y responder a las actividades informáticas malintencionadas dirigidas contra ella o sus Estados miembros, y es la primera vez que la Unión Europea ha utilizado este instrumento. El marco jurídico para la adopción de medidas restrictivas específicas en respuesta a los ataques informáticos se adoptó en mayo de 2019 y se renovó recientemente.

En los últimos años, la Unión viene acrecentando su resiliencia y su capacidad de prevención, disuasión y respuesta a las amenazas informáticas y las actividades cibernéticas malintencionadas, con el fin de salvaguardar la seguridad y los intereses europeos. En junio de 2017, la Unión Europea reforzó su respuesta estableciendo un Marco para una respuesta diplomática conjunta de la Unión a las actividades informáticas malintencionadas, el denominado "conjunto de instrumentos de ciberdiplomacia" (*vid supra* párrafo 33). Este Marco permite a la Unión Europea y sus Estados miembros recurrir a todas los instrumentos de la Política Exterior y de Seguridad Común (PESC), para actuar en la prevención, disuasión y respuesta a toda actividad informática malintencionada dirigida contra su integridad y su seguridad.

El Sistema adoptado por la Unión, dirigido a personas físicas o jurídicas, entidades u organismos, permite adoptar medidas restrictivas que contribuyan a la disuasión y a contrarrestar ataques cibernéticos al tiempo que evita la necesidad de atribuir dichos ataques a Estados con base en las normas de responsabilidad internacional[70], que presentan serios problemas de atribución, como ha subrayado ya la doctrina. A este respecto a la propia Decisión del Consejo mencionado señala que

> "Hay que diferenciar las medidas restrictivas específicas de la imputación de responsabilidad por los ciber ataques a un tercer Estado. La aplicación de medidas restrictivas específicas no implica tal imputación, que constituye una decisión política soberana adoptada en función de cada caso. Cada Estado miembro es libre de adoptar su propia determinación con respecto a la imputación de ciber ataques a un tercer estado" (Decisión [PESC] 2019/797, de 17 de mayo de 2019, considerando 9)

Lo cual no empece que en el caso de poder imputar a un Estado, en aplicación del Derecho Internacional de la Responsabilidad, una de estas actividades maliciosas, los Estados miembros de la Unión Europea y aún la misma Unión puedan, según ese Ordenamiento jurídico, recurrir a represalias o contramedidas contra el Estado mismo de acuerdo con las reglas del Derecho internacional que regulan esta figur [71].

2. Contramedidas, que regula el Derecho Internacional de la Responsabilidad, ¿son aplicables en caso de ciberataques?

2.1. El Derecho Internacional de la Responsabilidad

40. Durante muchos años, las relaciones internacionales se desarrollaron en un contexto de ausencia de instituciones centrales capaces de imponer coercitivamente, llegado el caso, el cumplimiento

Europea para promover la seguridad y la estabilidad internacionales en el ciberespacio", Comunicado de prensa 30 de julio de 2020 16:35 (https://www.consilium.europa.eu/es/press)

[70] CONSEJO DE LA UNIÓN EUROPEA, "La UE impone por primera vez sanciones en respuesta a los ciberataques", COMUNICADO DE PRENSA (Press office - General Secretariat of the Council), núm. 522/20, 30 de julio de 2020; Reglamento de ejecución (UE) 2020/1125 del Consejo, de 30 de julio de 2020, por el que se aplica el Reglamento (UE) 2019/796 relativo a medidas restrictivas contra los ciberataques que amenacen a la Unión o a sus Estados miembros, *Diario Oficial de la Unión Europea* L 246, de 30 de julio de 2020, pp. 4-9; Decisión (PESC) 2020/1127 del Consejo, de 30 de julio de 2020 por la que se modifica la Decisión (PESC) 2019/797 relativa a medidas restrictivas contra los ciberataques que amenacen a la Unión o a sus Estados miembros, *Diario Oficial de la Unión Europea* L 246, 30 julio 2020, pp. 12-181.

[71] *Vid*. M.Robles Carrillo, "Sanciones contra ciberataques: la acción de la Unión Europea", Instituto Español de Estudios Estratégicos (IEEE) Documento de Opinión 143/2020, 10 de noviembre de 2020, pp. 1-23; y para una reflexión jurídica en profundidad de estas medidas, PIERNAS LÓPEZ, J.J., *Ciberdiplomacia y Ciberdefensa en la Unión Europea*, *op. cit*. (nota 47 *supra*), pp. 102-140.

del Ordenamiento y sus principales sujetos, los Estados, autoprotegían sus derechos, y aun sus meros intereses, empleando para ello los procedimientos que estimaban más convenientes a sus propósitos)[72].

Tras la Segunda Guerra Mundial (1939-1945), la Carta de Naciones Unidas estableció, como sabemos, un auténtico sistema de seguridad colectiva apoyado en dos columnas:

— *Por un lado*, la prohibición del uso de la fuerza armada en las relaciones internacionales "salvo" en genuina y estricta legítima defensa y „sólo hasta" la intervención de Naciones Unidas (artículos 2.4 y 51).
— *Y, por otro,* el establecimiento de un dispositivo de reacción institucional contra el Estado que quebrantare injustificad mente la prohibición (capítulo VII: artículos 39-51), regido orgánicamente por el Consejo de Seguridad que ejerce la „responsabilidad primordial" en el tema y puede adoptar "decisiones" obligatorias (artículos 24 y 25).

El nuevo Sistema sustituye y acaba con el régimen basado en la autotutela del Derecho internacional clásico. Sólo la legítima defensa como respuesta a un ataque armado justifica el empleo unilateral de la fuerza militar por los Estados y en todo caso únicamente hasta el momento en que el Consejo de Seguridad adoptara las medidas pertinentes para el mantenimiento de La Paz.

Pero la Carta sigue amparando la legalidad de las represalias (hoy llamadas contramedidas); a cambio, ha condicionado y limitado severamente (en forma y fondo) su aplicación.

41. El Proyecto sobre la responsabilidad del Estado (2001)[73] consideró que las *contramedidas* eran una causa de exclusión de la ilicitud (artículo 22), reconociendo que el comportamiento antijurídico de un Estado A *para obligar a otro Estado B a que repare el perjuicio que le ha causado* pierde su carácter ilícito por ser una contramedida admitida (artículo 49.1)[74].

Por lo demás, la Comisión de Derecho Internacional ha considerado, en su Proyecto sobre las Organizaciones internacionales (2011)[75]:

> "que no existe ninguna razón de peso para excluir categóricamente" el que éstas puedan adoptar contramedidas o que sean objeto de las mismas (comentario 1 al artículo 51); del mismo modo ha entendido (en cuanto a su objeto y límites) que "no hay aparentemente nada que justifique distinguir a este respecto entre las contramedidas adoptadas contra organizaciones internacionales y las dirigidas contra Estados"[76].

42. Ya en 1996, al aprobar en primera lectura su Proyecto sobre la responsabilidad del Estado, la Comisión de Derecho Internacional se decantó por una concepción de las contramedidas "instrumental"

---

[72] Sobre las contramedidas en general, a la luz del Proyecto de artículos de la Comisión de Derecho Internacional sobre la responsabilidad del Estado por hechos internacionalmente ilícitos (2001, *vid. ad ex.* C.Gutiérrez Espada, *La responsabilidad internacional (consecuencias del ilícito)*, Diego Marin Ediciones, Murcia, 2005, pp. 164-218. Véase también *infra* nota 74.

[73] Texto del Proyecto de artículos sobre la responsabilidad del Estado por hechos internacionalmente ilícitos, *Informe de la Comisión de Derecho Internacional. 53 período de sesiones (23 de abril a 1 de junio y 2 de julio a 10 de agosto de 2001, Asamblea General. Documentos oficiales, 56 período de sesiones, suplemento núm. 19, A/56/10*, Naciones Unidas, Nueva York, 2001, pp. 1-591, pp. 21-405

[74] Sobre las contramedidas en el Derecho Internacional contemporáneo véase *supra* nota 72), asimismo, C.Gutiérrez Espada"La aplicación o ejecución forzosa del Derecho Internacional", *Teoría y metodología del Derecho. Estudios en homenaje al profesor Gregorio Peces-Barba. Volumen II*, Dykinson, Madrid, 2008, pp. 569-606; ID.: Función y límites de las represalias (o contramedidas) en el Derecho internacional contemporáneo", en *Estudios de Filosofía del Derecho y Fisolofía Política. Homenaje a Alberto Montoro Ballesteros,* Universidad de Murcia (DIGITUM-Murcia), 2013, pp. 555-575; C.Gutiérrez Espada /R.Bermejo García, "La responsabilidad patrimonial de los Estados en Derecho internacional", en Tomás Quintana López (director) y Anabelén Casares Marcos (coordinadora), *La responsabilidad patrimonial de la Administración Pública. Estudio general y ámbitos sectoriales*, tomos I y II, Tirant lo Blanc, Valencia, 2013 (2ª edición), tomo I, pp. 365-479, sobre todo pp. 444-460.

[75] "Texto del proyecto de artículos sobre la responsabilidad de las organizaciones internacionales con sus comentarios", *Informe de la Comisión de Derecho Internacional 63o período de sesiones (26 de abril a 3 de junio y 4 de julio a 12 de agosto de 2011). Asamblea General, Documentos Oficiales, Sexagésimo sexto período de sesiones, Suplemento núm. 10 (A/66/10)*, Naciones Unidas, Nueva York, 2011, pp. 1-394, pp. 55-184.

[76] Párrafo 5 del comentario al artículo 54.

y no "punitiva"; y un año después (asunto *Gabcíkovo-Nagymaros*) el Tribunal Internacional de Justicia remachó la idea al darla por hecho en la regulación que el Derecho vigente hacía de las mismas[77]. La Comisión hizo suyo este planteamiento tanto en el Proyecto sobre la responsabilidad del Estado (2001) como, en el año 2011, al aprobar de manera definitiva el relativo a la responsabilidad de las Organizaciones internacionales:

> "el Estado lesionado o la organización internacional lesionada *solamente* podrá adoptar contramedidas contra una organización internacional responsable de un hecho internacionalmente ilícito con el *objeto de inducirla a cumplir las obligaciones que le incumben de acuerdo con lo dispuesto en la tercera parte*" (artículo 51) (esto es, la obligación de reparar).

Descarta así la Comisión la tesis, presente en una fase anterior de sus trabajos, de que las represalias pudieran jugar, respecto de ciertos ilícitos, una función punitiva desde la comisión misma de la violación, idea mantenida en su día por el Relator del tema Roberto Ago y defendida aún por algunos internacionalistas. El efecto cumulativo de las posiciones de la Comisión (1996, 2001 y 2011) y del Tribunal Internacional de Justicia (1997) parece determinante para entender que la tesis que ve en las contramedidas un "modo de hacer efectiva la responsabilidad" y no una de las consecuencias de la comisión de un hecho ilícito, es la que "refleja la opinión general sobre el estado actual del Derecho [78].

En suma, las contramedidas son una reacción, contraria al Derecho internacional, que este "justifica" con el fin de que los Estados u Organizaciones internacionales *lesionados* por un hecho ilícito (y en ciertos supuestos también Estados u organizaciones *terceros*) fuercen al culpable a pechar con las consecuencias que el Derecho Internacional reserva para quienes quebrantan sus normas.

En todo caso, el Derecho internacional acoge esta figura, con el cuidado de mantener un equilibrio entre su *aceptación* (reflejo de una innegable realidad e instrumento que puede coadyuvar a la aplicación efectiva de las normas primarias y aun de las secundarias del Derecho internacional) y la *conveniencia de evitar abusos* en su aplicación. Impone por ello al Estado u Organización lesionados (y, en su caso, a los terceros habilitados) el *cumplimiento de toda una serie de condiciones o requisitos de tipo "procesal*" así como de ámbitos prohibidos a su acción:

A) *En cuanto a las exigencias previas a su adopción*, las contramedidas sólo pueden ir dirigidas contra el autor del hecho que causó un perjuicio a quien las desencadena, no contra terceros. Un Estado o una Organización internacional que quieran adoptar contramedidas contra otro Estado u Organización deben *requerirle* para que haga frente a su responsabilidad, *notificarle* que de no hacerlo tomará represalias, y en fin *ofrecerle negociaciones.*

Pese a que, en el marco del Proyecto sobre la responsabilidad del Estado (2001), algún miembro de la Comisión de Derecho Internacional consideró prematura la notificación de las contramedidas antes de que se hubieran celebrado negociaciones, pues sería contraproducente informar al Estado responsable de las medidas concretas que iban a adoptarse, el Comité de Redacción estimó que „era útil" y no resultaba "excesivamente gravosa para el Estado lesionado"; y en su Proyecto sobre la responsabilidad de las Organizaciones (2011) lo ha ratificado (artículo 55.1 y 2 y párrafo 2 del comentario).

Por otro lado, algunos países parecían rechazar incluso la exigencia del requerimiento previo, pero la Comisión de Derecho Internacional la mantuvo, entendiendo que este requisito ("conminación") "parece también reflejar una práctica general [79].

---

[77] Párrafo 2 del comentario al artículo 47, *Yearbook of the International Law Comission* 1996, II, Part. Two; sentencia de 25 de septiembre de 1997, *International Court of Justice Reports 1997*, pp. 7 ss., pp. 56-57, párrafo 87.

[78] INTERNATIONAL LAW ASSOCIATION: *First Report of the ILA Study Group pon the Law of State Responsibility (Submitted by the Chair of the Study Group to the Special Rappoteur and the Chair of the United Nations International Law Commission and the ILA Director of Studies,* P. Malanczuyk, Chairman, La Haya, 8 june 2000, pp. 1-55, pp. 25-26, párrafo 84 (http://www.ila.hq.org]).

[79] Párrafo 3 del comentario al artículo 52 del Proyecto de 2001, ratific ndose en el requisito en su Proyecto de 2011 sobre las Organizaciones (artículo. 54.1 y comentario 2 al mismo).

Si la oferta de negociación es atendida, se abre la puerta a la adopción de contramedidas. Incluso aunque se negocie y mientras un órgano o tribunal ante el que el asunto ha sido sometido no haya tomado alguna decisión al respecto vinculante (provisional o definitiva), aquéllas son posibles. El intento de algunos miembros de la Comisión de que se prohibieran, durante las negociaciones, todo tipo de represalias fue rechazado sobre la base de que esta posición no se había aceptado por el tribunal arbitral en el caso del *Acuerdo relativo a los Servicios Aéreos*[80]. La Comisión de Derecho Internacional descartó, pues, ir más allá de lo que el Derecho internacional general establece, negándose a prohibir las represalias mientras dos sujetos (Estados u Organizaciones internacionales) están negociando[81].

B) El condicionamiento formal o procesal de las contramedidas en el Derecho internacional no se reduce a una serie de exigencias previas a su desencadenamiento, sino que *opera también en cuanto a la forma de ejercerlas* ***in actu*** (las contramedidas deben ser proporcionadas).

La Comisión de Derecho Internacional exigió *expressis verbis* (artículo 51 del Proyecto de 2001 y artículo 54 del relativo a las Organizaciones de 2011) tres criterios para medir la proporcionalidad: el *perjuicio sufrido*, la *gravedad del hecho ilícito* y el *impacto de la contramedida sobre "los derechos en cuestió*n", explicándose (respecto de esta última frase) que con ella se recogen los términos empleados por el Tribunal Internacional de Justicia en el asunto *Gabcíkovo* (1997) y que alude tanto a los derechos del Estado (o en su caso Organización internacional) lesionado como a los del Estado (u Organización) autores del ilícito, pudiendo abarcar además los derechos de otros Estados (u Organizaciones) susceptibles de ser afectados[82].

En el caso de las Organizaciones internacionales, si el hecho ilícito lesiona directamente a la Organización como tal, es ésta (y no Estados sus miembros) la que puede adoptar contramedidas; pero si resultaron lesionados tanto la Organización como sus Estados y Organizaciones miembros, la regla de la proporcionalidad debe aplicarse igualmente, lo que llevaría a evitar "reacciones excesivas" (comentario 4 al art. 54).

C) Ni por Estados ni por Organizaciones internacionales, en fin, cabe la adopción de contramedidas que impliquen desconocer la prohibición del uso de la fuerza armada en las relaciones internacionales, las obligaciones establecidas para la protección de los derechos humanos fundamentales, las de carácter humanitario que prohíben las represalias, ni, en general, las que supongan desconocer cualquier obligación imperativa[83]. La jurisprudencia internacional ha ratificado esta disposición en su aplicación entre Estados[84].

Tampoco puede una Organización internacional (ni un Estado) suspender, ni siquiera como contramedida:

---

[80] Sentencia de 9 de diciembre de 1978, párrafo 91, *Report of International Arbitral Awards,* Naciones Unidas, vol. XVIII, 2006, pp. 417 ss.

[81] Artículo. 52.3 y 4 del Proyecto sobre la responsabilidad del Estado y comentarios 7 a 9 del mismo; y artículo 55.3 y 4 del Proyecto sobre las Organizaciones internacionales y comentario 3.

[82] Artículo. 51 y comentarios 1 a 7 del Proyecto de 2001; el artículo 54 del Proyecto sobre las Organizaciones internacionales es más sucinto, pero sus comentarios revelan que la CDI aplica a estas las mismas ideas que maneja el mencionado artículo 51.

[83] Artículo. 50.1, letras a) a d) y comentarios núm. 2-10 del Proyecto sobre la responsabilidad de los Estados y artículo 53.1, letras a) a d) y comentario 1 al Proyecto sobre la responsabilidad de las Organizaciones.

[84] Así, el Tribunal Penal Internacional para la antigua Yugoslavia en el asunto *Kupresic y otros* señaló expresamente con referencia a uno de ellos: "las represalias que consisten en la matanza de personas inocentes elegidas al azar, sin pruebas de su culpabilidad ni juicio alguno, son sin duda una violación fragrante de los principios más básicos relativos a los derechos humanos" (sentencia de 14 de enero de 2000 de la Sala de Primeras Instancia, *Prosecutor v. Zoran Kupresic, Mirjian Kupresic, Vlatko Kupresic, Drago Jasipovic, Dragan Papic, Vladimirr Cantic /"Lasva Valley"),* causa N.IT-95-16-T, párrafo 529).

Y en el caso de los *Prisioneros de guerra*, de la Comisión de Reclamaciones entre Etiopía y Eritrea, también se hizo lo propio incluso con mayor concreción: "La suspensión por Etiopía de los intercambios de prisioneros de guerra no puede justificarse... como contramedida..., ya que, como destaca el artículo 50 de los artículos de la Comisión de Derecho Internacional..., dichas medidas no pueden afectar a 'las obligaciones establecidas para la protección de los derechos humanos fundamentales' ni a 'las obligaciones de carácter humanitario que prohíben las represalias'" (Laudo parcial de 1 de julio de 2003, *Prisioners of War. Eritrea's claim 17*, párrafo 159).

— De un lado, las obligaciones que tuvieren en virtud de un procedimiento de arreglo de controversias con el Estado o la Organización internacional autores del hecho ilícito previo. Esta disposición se refiere a los procedimientos de arreglo relacionados con la controversia en cuestión y no con otros problemas que pudieran enfrentar a los Estados u Organizaciones internacionales implicadas y no tuviesen conexión con el conflicto en concreto que da lugar a las contramedidas. Dichos procedimientos serían aplicables pues y pertinentes tanto respecto de la controversia inicial sobre un hecho ilícito como en relación con el tema de si las contramedidas adoptadas como respuesta son o no legítimas (artículo 53.2. a) del Proyecto de 2011).
— Y, de otro, tampoco pueden incumplirse, ni siquiera como contramedidas, las obligaciones a cargo del Estado o de la Organización internacional lesionados que protejan la inviolabilidad de las misiones diplomáticas o consulares del Estado y su personal o la de los agentes, locales, archivos y documentos de la organización internacional autores del ilícito, pues de no ser así resultaría perjudicada la institución misma de las relaciones diplomáticas y consulares que, por su importancia y función, debe preservarse siempre[85].

Por lo demás, y aunque está claro que en su tenor literal esta restricción sobre el derecho a la adopción de represalias que tienen Estados y Organizaciones internacionales "es claramente inaplicable a las organizaciones internacionales" el razonamiento de fondo en que la misma se basa sí lo es, de modo que la Comisión de Derecho Internacional ha entendido igualmente que un Estado o una Organización no pueden, como contramedida, dejar de cumplir las obligaciones sobre la inviolabilidad de los agentes de una organización internacional, sus locales, archivos y documentos que respecto de ella tengan[86].

43. A la luz, por todo ello, de la doctrina de la Comisión de Derecho Internacional en sus Proyectos sobre la responsabilidad de los Estados (2001) y de las Organizaciones internacionales (2011), así como por el Tribunal Internacional de Justicia en el asunto *Gabcíkovo-Nagymaros*[87], las contramedidas se caracterizan en el Derecho internacional vigente por las siguientes notas:

— Se trata de comportamientos contrarios *prima facie* al Derecho internacional que se adoptan como respuesta a un hecho ilícito previo.
— Su única finalidad es la de incitar al autor del mismo a que cumpla las obligaciones que el Derecho Internacional de la Responsabilidad le impone, por lo que deben ir precedidas de un requerimiento al efecto al Estado responsable; las contramedidas, pues, deben ser reversibles, para que una vez el Estado responsable haya hecho frente a su deber pueda ser restablecida la situación anterior a la violación.
— Salvo las estrictamente provisionales y urgentes para la preservación de sus derechos, no pueden adoptarse contramedidas sin el requerimiento y la oferta de negociación apuntadas, no siendo por lo demás posibles (y de haberse desencadenado ya deben suspenderse) desde que el asunto se encuentre en manos de un tribunal capacitado para adoptar decisiones vinculantes y este ha decidido ya medidas cautelares o provisionales asimismo obligatorias.
— Las contramedidas deben ser proporcionales al perjuicio sufrido.
— No pueden en ningún caso lanzarse contramedidas que incumplan las que la Comisión de Derecho Internacional llamó "obligaciones sacrosantas" que se recogen en el Proyecto sobre la responsabilidad de los Estados (2001) y en el que regula la responsabilidad de las Organizaciones (2011)[88].

[85] Artículo 50.2.b y comentarios 14-15 del Proyecto sobre la responsabilidad del Estado.
[86] Artículo 53.2.b) y comentario 2 del Proyecto sobre la responsabilidad de las organizaciones internacionales.
[87] Sentencia de 25 de septiembre de 1997, *International Court of Justice Reports 1997*, pp. 7 ss., pp. 55-57.
[88] Párrafo 1 del comentario al artículo 50 de aquél y artículo 53 con sus comentarios de éste.

44. En el Derecho internacional clásico, las represalias sólo podían adoptarse por un *Estado lesionado*, esto es, el afectado directamente por el hecho internacionalmente ilícito de otro[89], pero el Derecho internacional contemporáneo cuenta, como sabemos (y además de las obligaciones "bilaterales"), con aquellas otras que sus sujetos contraen para con un "grupo de Estados" o para con la "comunidad internacional en su conjunto"[90]. Siendo esto así, la violación de estas obligaciones no debería generar las mismas consecuencias que las derivadas de las que ligan únicamente a dos sujetos del Derecho internacional.

La clave son los artículos 48 del Proyecto sobre la responsabilidad del Estado (2001) y el 49 del relativo a las Organizaciones (2011); en ambos, se faculta a Estados u Organizaciones internacionales no lesionados a invocar la responsabilidad del autor de un ilícito si la obligación incumplida es "colectiva" o existente "con relación a la comunidad internacional en su conjunto"[91].

A) Dado que la Comisión de Derecho Internacional aceptó, en su Proyecto sobre la responsabilidad del Estado (2001), que los Estados no afectados directamente por un ilícito ven, sin embargo, conculcados también sus derechos por la violación de ciertas obligaciones internacionales y puesto que, como sabemos, los Estados directamente lesionados pueden, si el responsable no quiere hacer frente a sus obligaciones, aplicarle contramedidas (artículos 49-53), surgió la duda de si el Derecho internacional permitiría, asimismo, a Estados no directamente afectados por el ilícito de otro, y renuentes a purgar éste jurídicamente, la adopción de contramedidas. El supuesto límite, claro, era el de la violación de una norma imperativa puesto que éstas podrían ser, en caso tal, universales. La Comisión contestó afirmativament dicha interrogante en el texto del Proyecto de artículos que aprobó provisionalmente en agosto del 2000[92].

La hostilidad, sin embargo, de algunos de sus miembros a esta disposición fue tan notoria como la de diversos Estados en la Sexta Comisión de la Asamblea General de Naciones Unidas, forzando a la Comisión a renunciar a la decisión que había, provisionalmente, adoptado. Y esta, finalmente, vino a decir: si según el Derecho internacional del momento, los Estados no directamente lesionados por un ilícito están capacitados para adoptar contramedidas en interés de los beneficiarios de la obligación que lo hagan, pero de no es así no podrán hacerlo… Esto es, a la postre, lo que transmite el artículo 54 del Proyecto de artículos (2001):

> "Este Capítulo no prejuzga el derecho de cualquier Estado [u organización internacional], facultado por el párrafo 1 del artículo 48 para invocar la responsabilidad de otro Estado, a tomar medidas lícitas contra este Estado para asegurar la cesación de la violación, y la reparación en interés del Estado lesionado o de los beneficiarios de la obligación violada"

A la postre, entonces, "un compromiso que pretende… dejar la solución del tema a futuros desarrollos del Derecho internacional y de la práctica"[93].

---

[89] Párrafos 1 y 8 de los comentarios introductorios al capítulo II de la Tercera parte del Proyecto sobre la responsabilidad del Estado por hechos internacionalmente ilícitos de 2001.

[90] Artículo 33.1 del Proyecto sobre la responsabilidad del Estado (2001) y del relativo a las Organizaciones internacionales (2011).

[91] *Vid. ad ex*. C.Gutiérrez Espada, Actio popularis en Derecho Internacional?", *Estudios de Derecho Internacional en Homenaje al Profesor Ernesto J. Rey Caro*, Editorial Marcos Lerner-Editora Córdoba, edición de Drnas Zlata-Lerner Marcelo y coordinación de Drnas Zlata., Córdoba (República Argentina), 2002, tomo I, pp. 549-575; ID.: "Las contramedidas de Estados 'terceros' por violación de ciertas obligaciones internacionales", *Anuario Argentino de Derecho Internacional*, vol. XI (2001-2002), pp. 15-49.

[92] El artículo 54 (*contramedidas tomadas por Estados que no sean lesionados*) decía:

"1. Todo Estado que esté habilitado en virtud del párrafo 1 del artículo 49 para invocar la responsabilidad de otro Estado podrá tomar contramedidas a petición y por cuenta de cualquier Estado que haya sido lesionado por la violación, en la medida en que este último Estado esté a su vez habilitado para tomar contramedidas en virtud del presente capítulo.

2. En los casos a que se hace referencia en el artículo 41 [19], cualquier Estado estará habilitado para tomar contramedidas, de conformidad con lo dispuesto en el presente capítulo, en interés de los beneficiarios de la obligación violada

3. Cuando más de un Estado tomen contramedidas, los Estados involucrados cooperarán a fin de que se cumplan las condiciones establecidas por el presente capítulo para la adopción de contramedidas" (A/CN.4/L.600, 21 de agosto de 2000, p. 21).

[93] J.Crawford, *State responsability. General Part*, Cambridge University Press, Cambridge, 2014 (3ª impresión de la 1ª ed.), p. 706.

En suma, la Comisión de Derecho Internacional sustituyó su intento por ofrecer *de lege ferenda* una *regulación* equilibrada entre la *conveniencia de* no desarrollar demasiado progresivamente el Derecho de la Responsabilidad y la *necesidad* de asumir que las consecuencias de la violación de obligaciones multilaterales (en especial las debidas a la comunidad internacional en su conjunto) no pueden ser las mismas que las que se derivan de la de una obligación bilateral; sustituyó, decimos, ese intento[94], por una *cláusula de salvaguardia* (idea del Reino Unido), con la que la Comisión *se lava las manos respecto de esta particular cuestión*. La decisión, en una oportunidad crítica como ésta y después de tantos años de trabajo, de posponer el paso adelante que hubiera iluminado el tema de las contramedidas de terceros en caso de violación grave del Derecho internacional, ya respecto de un Estado ya en relación con víctimas no estatales (como los seres humanos y sus derechos), no me parece acertada. ¿No era acaso posible aceptar en un texto de esta naturaleza lo que hace más de 20 años reconoció el Instituto de Derecho internacional?, esto es, que en el supuesto de violaciones gravísimas por un Estado de los derechos humanos, otros pueden adoptar contramedidas no armadas[95]; ¿no era posible, dicho esto, exigir una mínima coordinación? ¿Es mejor callar, y que una situación incierta regule los hechos?

Tal vez es cierto que la práctica existente no resultaba definitiva. El examen que el Relator Crawford llevó a cabo sobre la adopción de „medidas" que Estados no directamente lesionados habían desencadenado contra otro al que se considera culpable de violar obligaciones establecidas para con la comunidad internacional en su conjunto, la condujo a una valoración cautelosa por varias razones[96]. Para la Comisión de Derecho Internacional misma, esta práctica es „incierta", „escasa y concerniente a un número limitado de Estados"; de ahí que concluya entendiendo que:

> "en la actualidad no parece reconocerse claramente el derecho de los Estados mencionados en el artículo 48 a adoptar contramedidas en interés colectivo", por lo que „en consecuencia, no es apropiado incluir en los presentes artículos..."[97].

Hay quien ha apoyado esta decisión[98]. Para mí, se trata, pura y simplemente, de una "huida hacia delante[99].

---

[94] "Que buscaba *limitar* y no expandir las circunstancias en que estas [contramedidas de terceros] podían adoptarse" (J.Crawford *State responsability. General Part*, *op. cit.* [nota 93 *supra*], p. 705)

[95] Resolución de Santiago de Compostela de 13 de septiembre de 1989 sobre la *protección de los derechos humanos y el principio de no intervención en los asuntos internos de los Estados*, artículo 2, párrafos 2º y 3º) (disponible en www.idi-iil.org).

[96] La práctica estaba dominada por un grupo de Estados (el occidental); era selectiva, pues en casos similares a los que provocaron la "intervención" nada se hizo; y no siempre era posible justificar las reacciones de los Estados terceros como"contramedidas", sino más bien como actos de mera "retorsión" o, incluso, cobijándose bajo la figura del "cambio de circunstancias" como causa de denuncia, terminación o suspensión de los tratados (Comisión de Derecho Internacional, párrafos 3-4 del comentario al artículo 54).

[97] Párrafos 3 y 6 del comentario de la Comisión de Derecho Internacional al artículo 54 de su Proyecto sobre la responsabilidad del Estado por hechos internacionalmente ilícitos (2001).

[98] Considerando que sería peligroso codificar las que este autor llama "medidas de solidaridad" en un mundo fragmentado, pues "daría a los actores poderosos demasiado fácilmente la posibilidad de regularizar como policial su posición". Para el internacionalista finlandés, bastaría con tolerar el que un Estado recurra a medios formalmente ilegales para responder a violaciones ominosas de intereses comunitarios importantes, pero sin "juridificar" la tolerancia; así, sería la reacción de la comunidad ante una práctica, que seguiría siendo formalmente ilegal, la que fuera depurando qué conviene codificar y qué no (M.Koskenniemi, "Solidarity measures: State responsibility as a new international order", *British Yearbook of International Law,* LXXII [2001], pp. 337-356).

[99] Existe hoy una tendencia clara y, con toda probabilidad, no únicamente tan "occidental" como la Comisión de Derecho Internacional afirma (¿o es que no la han practicado también los Estados africanos respecto de una Sudáfrica con un régimen que aplicaba el *apartheid*?). Por todo ello, parecía razonable regular mediante una norma *de lege ferenda* esta zona gris. Dado que en relación con las crisis humanitarias más graves no podemos ver en Naciones Unidas un socio (siempre) fiable, el cese de genocidios o limpiezas étnicas hubiera podido encontrar en una regulación de las contramedidas un arma considerable, capaz acaso de provocar la reacción institucional, preferible sin duda, de la ONU; sobre todo ahora que el reconocimiento (2005) por el Secretario General de Naciones Unidas de la existencia de una *obligación internacional de proteger*, a cargo llegado el caso de la comunidad internacional en su conjunto, que habilitara a esta a adoptar las medidas necesarias, por medio del Consejo de Seguridad de dicha Organización, para impedir catástrofes humanitarias del tipo de los genocidios o las "limpiezas étnicas", parece irse disolviendo (…).

Más aún, si el artículo 41.1 impone a todos el deber de cooperar para poner fin, por medios lícitos, a una violación grave de obligaciones emanadas de normas imperativas del Derecho internacional general (a las que se refiere el art. 40), ¿no

B) En el Proyecto sobre la responsabilidad de las Organizaciones internacionales (2011), la Comisión ha mantenido la regulación prevista para los Estados sobre esta cuestión, estableciendo que sus disposiciones no prejuzgan el derecho de los Estados y Organizaciones internacionales no lesionados, en caso de violación de obligaciones colectivas o para con la comunidad internacional en su conjunto, para adoptar contramedidas contra el Estado u Organización autores de tal violación (artículo 57).

En definitiva, no parecía llegado el momento de poder afirmar con la rotundidad necesaria que la práctica en esta cuestión tuviese la amplitud y, acaso, la precisión suficientes para haber generado ya, sin la menor sombra de duda, una norma de Derecho internacional general. El profesor Crawford, Relator Especial del tema en su etapa definitiva, todavía creía que

> "el análisis de la práctica estatal sobre el recurso a contramedidas colectivas no conduce a conclusiones claras"[100].

Y, no obstante, véase, también, *infra* párrafo 51 *in fine*.

45. Es mi intuición que, lenta pero inexorablemente, esta posición irá cambiando (de nuevo, véase *infra* párrafo 51 *in fine*).

Me ha llamado poderosamente la atención, en este sentido, la magnífica reflexión que sobre la aplicación de las contramedidas de Derecho internacional a las actividades de los Estados en el ciberespacio efectuó el Gobierno de Nueva Zelanda, en su declaración sobre el tema de 1 de diciembre de 2020.

Vuelvo sobre ella. A continuación, en el contexto en el que dicha declaración se hizo, cuando me refiera a las contramedidas en el *Manual de Tallinn 2.0*.

2.2. El Manual de Tallinn 2.0

46. El Manual asume básicamente la regulación de las represalias del Derecho internacional. Las considera (cibernéticas o no) causa de exclusión de la ilicitud[101].

En él, su autor, el Grupo Internacional de Expertos defiende que las contramedidas no son invocables frente a ciberoperaciones de actores no estatales[102]. Piensa que el Derecho internacional impone obligaciones (como las de respetar su soberanía o la de la prohibición de la fuerza armada) a los Estados únicamente y no a los actores no estatales; no quiere decir con ello que las ciber operaciones de esos grupos sean lícitas (probablemente violarían el Derecho interno del Estado objeto de las ciberoperaciones). Y en todo caso, el Estado atacado podría encontrar una causa de exclusión de la ilicitud que justificase medidas contra el actor no estatal (necesidad o legítima defensa)[103]. Como llama la atención que estas dos causas de exclusión de la ilicitud sean aplicables y no las contramedidas, el Grupo de Expertos probablemente (pienso) ha descubierto que las causas que sí pueden lo permitirían por su texto y las contramedidas no:

— La necesidad porque el peligro que lo provoca no tiene por qué provenir de otro Estado:

> "contrariamente a las contramedidas (Regla 20), la necesidad no depende de una conducta ilícita previa de otro Estado. El estado de necesidad puede ser causado por un desastre natural u otra situación que no tenga que ver con normas jurídicas internacionales"[104].

---

tendrían, entonces, todos los Estados en disposición de hacerlo que adoptar contramedidas (no armadas) si ello resultase necesario para conseguirlo?

[100] J.Crawford, *State responsability. General Part*, op.cit. (*supra* nota 93), p. 703.

[101] M.N.Schmitt, (General editor), *Tallinn Manual 2.0 on the International Law applicable to cyber operations, prepared by the International Group of Experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence,* Cambridge University Press, Cambridge, 2017, regla 20, pp. 111-116

[102] *Ibidem*, p. 113, comentario 7.

[103] M.N.Schmitt (General editor), *Tallinn Manual 2.0 ... op. cit.* (nota 101 *supra*), p. 114, comentario 10.

[104] *Ibidem*, p. 137, regla 26, comentario 9.

— La legítima defensa, porque el artículo 51 de la Carta no exige específicamente que su desencadenante (el ataque armado) sea obra, necesariamente, de un Estado. Tesis de Koijmann y Simma en los asuntos del Muro (2004) y de las actividades armadas en el territorio del Congo (2005), que la mayoría del Grupo Internacional de Expertos comparte[105].
Repárese que el Grupo parece aceptar la doctrina *unable or unwilling State*...[106] y que en todo caso (la mayoría) defiende la invocación de la legítima defensa frente a actores no estatales en otro Estado.

En todo caso, los Expertos reconocieron que existe la tesis de quienes creen que las contramedidas sí pueden aplicarse a los actores no estatales, sobre todo en los casos en los que ningún Estado podría ser acusado de un hecho ilícito[107].

47. El Manual considera que las contramedidas son, en el ámbito de las actividades en el ciberespacio, causas de exclusión de la ilicitud que tienen el mismo objetivo y naturaleza que en el Derecho Internacional de la Responsabilidad, esto es, forzar al Estado autor del hecho ilícito previo a hacer frente a su responsabilidad[108].

Más recientemente, la Declaración del gobierno de Nueva Zelanda sobre el tema expone con mucha claridad esta posición[109].

---

[105] *Ibidem*, p. 345, regla 71, comentario 19.

[106] Cuyo contenido describe muy bien el Informe con el que la Administración Obama, en los Estados Unidos, se despidió de la Casa Blanca: " Los Estados, de conformidad con el derecho de legítima defensa individual o colectiva, cuando se enfrentan a un ataque armado *in actu* o inminente por grupos armados no estatales y el uso de la fuerza resulta necesario a causa de que el gobierno del Estado en el que la amenaza se localiza es incapaz o no desea prohibir el uso de su territorio a los actores no estatales en particular para llevar a cabo esos ataques (…) [pueden actuar] en legítima defensa contra los actores no estatales en el territorio de ese estado sin su consentimiento"; precisando, además, que esta posibilidad está admitida "por el derecho internacional consuetudinario" (*Report on the legal and policy framework guiding the United States'use of military force and related national security operations,* The White House, december 2016, pp. 1-61, pp. 9-10. Sobre esta doctrina véase, Mª. J. Cervell Hortal, *La legítima defensa en el Derecho Internacional contemporáneo (Nuevos tiempos, nuevos actores, nuevos retos),* Tirant lo Blanch, Valencia, 2017, pp. 228-237; ID., "Sobre la doctrina *unwilling or unable State* (podría el fin justifica los medios?)", *Revista Española de Derecho Internacional,* vol. 70, núm. 1, 2018, pp. 77-100; ID., *La defensa contra sistemas aéreos no tripulados (C-UAS): una reflexión jurídica preliminar desde el punto de vista del uso de la fuerza*, Documento de Investigación 11/2018, Instituto Español de Estudios Estratégicos, julio 2018 (https://www.ieee.es), pp. 1-30, p. 23.

[107] " Considérese un caso en el que un grupo terrorista situado en un Estado lanza ciber operaciones contra otro Estado, y las operaciones resultan en daños físicos al hardware en territorio de este último. Si dicha operación hubiera sido conducida por un Estado habría, como mínimo, violado su soberanía (Regla 4). El primer Estado toma todas las medidas posibles para poner fin a las operaciones del grupo que se originan en su territorio de acuerdo con su deber de ejercer la debida diligencia (Reglas 6-7), pero finalmente fracasa y las operaciones persisten. El Estado blanco de los ciberataques, que continúa sufriendo daños a causa de las actividades del grupo, puede, según los defensores de esta tesis, de adoptar contramedidas contra el grupo incluso aunque estas medidas puedan violar la soberanía del primer Estado" (SCHMITT, M.N. [General editor], *Tallinn Manual 2.0 ..., op. cit.* [nota 101 *supra*], pp. 113-114, comentario 8 a la regla 20).

[108] *Ibidem*, regla 21, pp. 116-122.

[109] "18. Regardless of whether the activity amounts to an internationally wrongful act, a state may always attribute *political* responsibility for malicious state cyber activity and may always respond with retorsion (i.e. unfriendly acts not inconsistent with international law).

19. Where a state is subject to cyber activity that amounts to an internationally wrongful act, it may also invoke the international *legal* responsibility of the responsible state. States are responsible for internationally wrongful acts that can be attributed to them, including wrongful cyber activities. An internationally wrongful act can be attributed to a state if it was carried out by organs of the state, persons or entities empowered to exercise elements of governmental authority on behalf of that state, or agents acting on the instructions of, or under the direction or control of the state; or where the state acknowledges and adopts the act as its own. States may also be internationally responsible for aiding or assisting internationally wrongful cyber activity carried out by another state.

20. States should act in good faith and take care when attributing legal responsibility to another state for malicious cyber activity. While international law prescribes no clear evidential standard for attributing legal responsibility for internationally wrongful acts, a victim state must be sufficiently confident of the identity of the state responsible. What constitutes sufficient confidence in any case will depend on the facts and nature of the activity. While any legal attribution should be underpinned by a sound evidential basis, there is no general obligation on the attributing state to disclose that basis. However, a state may choose as a matter of policy to disclose specific information that it considered in making its attribution decision, and may be required to defend any such decision as part of international legal proceedings.

El Grupo de Expertos estuvo de acuerdo con el requisito exigido por la Comisión de Derecho Internacional de que, antes de lanzar contramedidas, el Estado debe notificar al Estado contra el que van a adoptarse que haga frente a su responsabilidad, advirtiéndole que de no hacerlo así deberá soportar represalias. Los Expertos piensan, además, que (en el caso particular de las ciberoperaciones) la exigencia resulta especialmente adecuada porque es posible, con relativa facilidad, que el origen del ciberataque sea falso o poco claro. En todo caso, el Grupo consideró altamente probable, en este tipo de operaciones, que no pueda cumplirse el requisito de la notificación, por el carácter urgente de las contramedidas que deben adoptarse a fin de evitar los daños pertinentes[110] (las contra medidas de carácter urgente, por lo demás, han sido reconocidos por la Comisión en su Proyecto de Artículos de 2001, artículo 52.2).

No obstante la mayoría del Grupo consideró conforme a Derecho, contrariamente a lo que sostiene el Proyecto de la Comisión (2001), la adopción de contramedidas antes de intentar negociaciones y aun mientras estas se llevan acabo. Acepta también la mayoría del Grupo que las contramedidas no deben iniciarse o, de haberse hecho, deben suspenderse una vez que la cuestión está en manos de un tribunal capacitado para adoptar decisiones jurídicamente vinculantes y la conducta ilícita ha cesado[111].

48. El Manual aplica también el Derecho Internacional de la Responsabilidad en relación con los requisitos que el Estado lesionado por el hecho ilícito de otro debe respetar, *antes* y *durante* la práctica de las contramedidas. Así:

A) No pueden adoptarse contramedidas que:

— Afecten a los derechos humanos, al menos a los derechos libertades fundamentales.
— Estén prohibidas por el Derecho Internacional Humanitario.
— Vulneren normas imperativas (el Manual cita el genocidio, precisando asimismo que aunque una minoría del Grupo Internacional de Expertos coincide con el Tribunal Penal Internacional para la antigua Yugoslavia en que la mayoría de normas de Derecho Internacional Humanitario son imperativas, la mayor parte de los expertos que conformaban el Grupo no lo veía así).
— Y deben respetar el Derecho Diplomático y Consular[112].

Hay una cuestión de interés sobre el uso de la fuerza (en principio, una norma imperativa) que me interesa aclarar. Si lo entiendo bien, una minoría del Grupo Internacional de Expertos defiende, con apoyo en la Opinión del juez Simma, del Tribunal Internacional de Justicia, en el asunto de la *plataformas petrolí*feras (2003), la licitud de las contramedidas que impliquen un "uso menor" de la fuerza (pues no violaría, pienso yo entienden los Expertos, el núcleo duro de la prohibición) frente a ciber ataques ilegales que no lleguen al umbral de ataque armado (y no dan, pues, lugar a la invocación del derecho de legítima defensa)[113].

21. If State A attributes internationally wrongful cyber activity to State B, State A may demand reparation and guarantees of non-repetition and/or utilise peaceful dispute resolution mechanism including the International Court of Justice where available. State A may also respond with countermeasures against State B (...)" (NEW ZEALAND, Foreign Affairs and Trade, Crown Law, *The application to International Law to State activity in Cyberspace*, 1 december 2020, pp. 1-4, pp. 3-4)..

[110] M.N.Schmitt (General editor), *Tallinn Manual 2.0 ..., op. cit.* (nota 101 *supra*), p. 120, regla 21, comentarios 10-11.

[111] *Ibidem,* pp. 120-121, regla 21, comentarios 13-14.

[112] M.N.Schmitt (General editor), *Tallinn Manual 2.0 ..., op. cit.* (nota 101 *supra*), pp. 122-126, regla 22, comentarios 3-8.

[113] "Según la mayoría del Grupo Internacional de Expertos, la obligación de abstenerse del uso de la fuerza es una limitación clave para un Estado lesionado mientras lleva a cabo contramedidas. Esta posición es consistente con la jurisprudencia del tribunal internacional de justicia [Corfu p. 35 y Nicaragua párrafo 249] y es replicada en el artículo 50 (1) (a) de los Artículos sobre Responsabilidad del Estado".

"Una minoría de expertos considero que contramedidas que impliquen un uso de la fuerza son apropiadas como respuesta a un uso ilícito de la fuerza que no puede ser calificado de ataque armado (sea por medios cibernéticos o no). Estos expertos se basaron en la opinión del juez Simma que defendió un derecho limitado a tomar contramedidas que impliquen uso de la fuerza frente a operaciones cibernética ilícitas que se sitúan a medio camino entre los usos menos graves de la fuerza y los calificados de ataque armado a los efectos del derecho de legítima defensa" (SCHMITT, M.N. General editor], *Tallinn Manual 2.0 ..., op. cit.* [nota 101 *supra*], pp. 125-126, regla 22, comentarios 11, 13-14).

B) Las contramedidas, cibernéticas o no, deben ser proporcionales al daño sufrido, como la Comisión de Derecho Internacional mantuvo en su Proyecto (2001):

> Pero "proporcionalidad no implica reciprocidad; no es necesario que las contramedidas del Estado lesionado violen la misma obligación quebrantada por el Estado responsable. Ni tampoco es obligado que las contramedidas sean de la misma naturaleza que el hecho internacionalmente ilícito subyacente que las justifica. Contramedidas no cibernéticas pueden ser usados como respuesta a un hecho internacionalmente ilícito que implica operaciones cibernética y viceversa. No obstante, por lo general el requisito de la proporcionalidad puede probablemente ser más fácilmente respetado, o al menos puede más fácilmente considerarse que ha sido respetado, cuando las contramedidas son del mismo tipo"[114].
>
> Nueva Zelanda, en su Documento de 1 de diciembre de 2020, acepta en esencia esta posición[115].

49. El *Manual de Tallinn 2.0,* en fin, no parece aprobar las eventuales represalias de terceros. Sólo los Estados lesionados pueden adoptar contramedidas, sean cibernética has o no:

> "Por ejemplo, una firma tecnológica de información no puedo actuar por su propia iniciativa para responder a una ciber operación dañosa que se llevó contra ella proclamando su respuesta con una contramedida. Para ilustrar la cuestión, Sony que sufrió ciberoperaciones maliciosos en 2014, que se atribuyeron a Corea del Norte, no estaba titulada para responder con un hackeo como contramedida según el Derecho de la Responsabilidad del Estado. El derecho de adoptar contramedidas se reserva a Estados Unidos, asumiendo que la operación contra Sony pudiera calificarse de un hecho internacionalmente ilícito (regla 14) de Corea del Norte contra Estados Unidos, por ejemplo por violación de su soberanía (regla 4)"[116].

Pero

> "Nada impide, sin embargo, a un Estado lesionado dirigirse a una firma privada, compañías extranjeras incluso, para adoptar en su nombre contramedidas frente a los Estados responsables. En este caso, las ciberoperaciones de la compañía serían, por lo general, imputables el Estado lesionado (regla 17). Las ciberoperaciones en cuestión estarían sujetas a todas las restricciones y condiciones relevantes condiciones de las contramedidas"[117].

No hubo acuerdo en el Grupo sobre si eran posibles las contramedidas de Estados no lesionados en casos de violación de obligaciones *erga omnes* (artículo 48.1 del Proyecto de la Comisión sobre la responsabilidad del Estado por hechos internacionalmente ilícitos de 2001)[118].

Aunque en relación con las obligaciones *erga omnes*, la regla 30 del Manual de Tallin 2.0[119] reconoce a cualquier Estado el derecho a invocar la responsabilidad de otro por ciberoperaciones que supongan la violación de obligaciones internacionales *erga omnes*, su texto parece limitarse a reconocer el derecho de invocar la responsabilidad, sin más. Y ello en dos sentidos:

---

[114] M.N.Schmitt [General editor], *Tallinn Manual 2.0 ..., op. cit.* ([nota 101 *supra*), pp. 128-129, regla 23, comentario 7.

[115] "Countermeasures are otherwise internationally wrongful acts that are permitted when undertaken to induce another state to comply with its obligations under international law. They may include, but are not limited to, cyber activities that would otherwise be prohibited by international law. Any countermeasure must:

a. be undertaken to induce compliance by the state in breach of international law;

b. be directed at the state responsible for the internationally wrongful act;

c. not rise to the level of use of force or breach peremptory norms of international law; and

d. be necessary and proportionate" (NEW ZEALAND, Foreign Affairs and Trade, Crown Law, *The application to International Law to State activity in Cyberspace*, *op. cit*. [nota 109 *supra*], apartado 21. Véase también los apartados 25 (International Humanitarian Law) y 26 (International Human Rights Law).

[116] M.N.Schmitt (General editor), *Tallinn Manual 2.0 ..., op. cit.* (nota 101), p. 130, regla 24, comentario 2.

[117] *Ibidem,* p. 131, regla 24, comentario 3.

[118] "No está regulado si los Estados a los que se refiere el artículo 48.1 pero no son directamente lesionados por el Estado responsable de un hecho internacionalmente ilícito hito pueden recurrir a contramedidas distintas de las medidas lícitas como la retorsión para conseguir el cese de la violación y la reparación en interés del Estado lesionado o de los beneficiarios de la obligación el grupo internacional de expertos no pudo conseguir consenso en este tema" (*Ibidem,* p. 131, regla 24, comentario 5).

[119] *Ibidem*, pp. 152-153 (como el artículo 48 del Proyecto de la CDI).

— De una parte, no descarta la regla del Derecho internacional de que un tercero solo podrá exigir al autor la reparación del hecho ilícito ante un órgano o tribunal con jurisdicción sobre el caso[120]
— De otra, y en relación a las eventuales contramedidas de Estados no lesionados directamente, se remite a la regla que regula las contramedidas en el Derecho internacional[121], y en la que no hubo acuerdo sobre las contramedidas de terceros.

Más fácil parece invocar al efecto la figura de la necesidad como respuest [122].

Se planteó y debatió, además, en particular si un Estado no lesionado podría adoptar contramedidas en apoyo de un Estado lesionado, si este le pide esta ayuda al efecto:

> "Algunos expertos eran de la opinión que un Estado no lesionado puede adaptar contramedidas como respuesta a un hecho internacionalmente ilícito cometido contra un Estado lesionado si este último se lo pide. Y basaron su punto de vista en cierta práctica estatal tal y como la identificó la Comisión de Derecho Internacional [párrafos 3 y 4 del comentario de la Comisión de Derecho Internacional al artículo 54]. La mayoría de los expertos sin embargo tomó la postura de que, como se regula en el juicio de Nicaragua [párrafo 249] las contramedidas tomadas en nombre de otro Estado son ilícitas. Estos expertos notaron que la comisión de derecho internacional indicó que la práctica arriba mencionada era 'escasa e implicaba a un número limitado de Estados'" [comentario 6 al artículo 54]"[123].

También se debatió si un Estado no lesionado puede prestar asistencia al Estado lesionado en las contramedidas que este mismo adopte en relación con el Estado responsable:

> "Aunque la mayoría era de la opinión de que los Estados no pueden lícitamente adoptar contramedidas el nombre de otro Estado, los miembro del grupo se dividieron sobre si el Estado podía prestar asistencia a otro en la adopción por este último de contramedidas. El problema se plantearía, por ejemplo, si un Estado aporta guía o cómo conducir un hackeo de respuesta que pueda calificarse como contramedida o información compartida en relación con las vulnerabilidades de la ciber infraestructura del Estado responsable".

Respecto de esta particular cuestión, los Expertos se dividieron en tres grupos:

> "no obstante lo cual, todos los expertos estuvieron de acuerdo en que si un Estado ayuda o asiste en una ciber operación que no consigue ser calificada como contramedida, puede ser considerado responsable por ayudar o asistir a un hecho internacionalmente ilícito (regla 18)"[124].

La reciente posición (1 diciembre 2020) del gobierno de Nueva Zelanda es muy clara: sí a la prestación de su ayuda a un Estado objeto de ciberataques, que lo solicite, en la adopción contra el Estado autor de contramedidas[125].

50. Conviene apuntar, en fin, por tener en cuenta la práctica internacional reciente, los casos del Reino Unido y de Francia.

---

[120] NEW ZEALAND, Foreign Affairs and Trade, Crown Law, *The application to International Law to State activity in Cyberspace*, op. cit. (nota 109 *supra*), apartado 22.

[121] M.N.Schmitt (General editor), *Tallinn Manual 2.0 ..., op. cit.* (nota 101*supra*), p. 152, regla 30, comentario 1.

[122] *Ibidem,* p. 152, regla 30, comentario 1 también.

[123] *Ibidem,* p. 132, regla 24, comentario 7.

[124] *Ibidem,* p. 132, regla 24, comentario 9 *in fine*.

[125] "Given the collective interest in the observance of international law in cyberspace, and the potential asymmetry between malicious and victim states, New Zealand is open to the proposition that victim states, in limited circumstances, may request assistance from other states in applying proportionate countermeasures to induce compliance by the state acting in breach of international law. In those circumstances, collective countermeasures would be subject to the same limitations set out above" (NEW ZEALAND, Foreign Affairs and Trade, Crown Law, *The application to International Law to State activity in Cyberspace*, op. cit. (nota 109 *supra*), apartado 22).

En 2016, el Concepto sobre Ciberdefensa del Reino Unido expuso tan sucinta como adecuadamente, la aplicación de estas normas del Derecho internacional en vigor a las actividades en el ciberespacio:

> "An internationally wrongful act commited by a state entitles the injures state to take proportionate countermeasures. Countermeasures are actions: In light of a refusal to remedy the wrongful act; directed against the other state to induce compliance with its obligations; and which are proportionate"[126].

Francia ha defendido (septiembre 2019), con mucha claridad, y de acuerdo con el Derecho Internacional de la Responsabilidad expuesto, su derecho a adoptar contramedidas "como respuesta a un ciberataque constitutivo de una violación del Derecho internacional (incluso el de un recurso a la fuerza) a fin de hacer respetar y proteger sus intereses y de forzar al Estado responsable a hacer frente a sus obligaciones"[127]. Añadiendo dos precisiones:

— Una:

> "elles [les contremésures] s'inscrivent, par conséquant, dans une réponse de nature pacifique et ont pour unique but la cessation de la violation initiale"

— Y, la segunda

> "L'Etat victime peut, dans certaines circonstances, déroger à l'obligation de notifier préalablement l'Etat responsable de la cyberopération, lorsqu'il existe une nécéssité à protéger ses droits. Cette possibilité d'adopter des contre-mesures urgentes est d'autant plus à propos dans le cyberespace étant donné la prédominance des procédés de dissimulation et les dificultés de traçabilité [128].

51. Una vez expuestas las disposiciones del Derecho Internacional de la Responsabilidad (centrándonos en el caso de las contramedidas) y la posición adoptada por el Manual de Tallin 2.0, es relevante destacar que la Comisión de Derecho Internacional se ha ratificado, en 2019, a propósito de "las normas imperativas de Derecho Internacional (*ius cogens*)", en dos cuestiones de interés de las que he hecho mención: ni *actio popularis* ni contramedidas de terceros.

A) Ni *actio popularis* (...). El párrafo 2 de la conclusión 17, con base en el artículo 48 del Proyecto de la Comisión de 2001, acepta la invocación por Estados no lesionados de la responsabilidad del Estado que haya violado obligaciones emanadas de normas imperativas[129].

Pero ya quedó claro en el Proyecto de conclusiones sobre las normas imperativas de Derecho internacional general (*ius cogens*) que el hecho de que la norma incumplida sea de *ius cogens* no es causa bastante para justificar la jurisdicción del tribunal ante el que eventualmente un Estado (lesionado o meramente habilitado) invoca la responsabilidad del autor del ilícito[130].

---

[126] MINISTRY OF DEFENCE (DEVELOPMENT, CONCEPTS AND DOCTRINE CENTRE). *Cyber Primer. Second edition, july 2016,* pp. 1-100, p. 12, apartado 1A.2 (del Anexo 1A. International law aspects) (https://www.gov.uk/mod/dcdc)

[127] MINISTÈRE DES ARMÉES. REPUBLIQUE FRANÇAISE, *Droit International appliqué aux opérations dans le cyberespace*, 9 de septiembre de 2019, pp. 1-18, p. 8 (https://www.defense.gouv.fr).

[128] MINISTÈRE DES ARMÉES. REPUBLIQUE FRANÇAISE, *Droit International appliqué aux opérations dans le cyberespace, op. cit.* (nota 127 *supra*), p. 8. Repárese en que Francia comparte la importancia de las contramedidas, dada la naturaleza de las mismas, en el ámbito en especial de las actividades en el ciberespacio, que el Grupo Internacional de Expertos que elaboró el Manual de Tallinn defendió (*supra* párrafo 46).

[129] *Vid.* C.Gutiérrez Espada, *De la alargada sombra del ius cogens*, Comares, Granada, 2021, pp. 4-9; también RUEDA FERNÁNDEZ, C., "La regulación jurídica de las violaciones graves de obligaciones esenciales emanadas de normas imperativas de Derecho internacional general en el Proyecto de artículos de la Comisión de Derecho Internacional", *Anuario de Acción Humanitaria y de Derechos Humanos,* Universidad de Deusto, núm. 2/2005, pp. 67-130, pp.105-110.

[130] *Vid*. C.Gutiérrez Espada, *De la alargada sombra del ius cogens*, *op. cit*. (nota 129 *supra*), pp. 52, 60-62, 143-144.

Hubo propuestas en otro sentido. Así, se expresó la opinión en el seno de la Comisión de que el Proyecto de conclusiones, dando un paso adelante en el desarrollo progresivo (opinión que el Informe de la Comisión recogió), respecto del proyecto de conclusión 14.2 del Relator, debía estipular:

> "que el consentimiento del Estado a la competencia del Tribunal Internacional de Justicia no era necesario en el caso de las controversias relativas al *ius cogens*"[131].

Y, por si las dudas, en efecto, el Sr. Cissé propuso *expressis verbis* un texto que, entiendo yo, viene a reconocer claramente el concepto de *actio popularis*:

> "En vista de las observaciones que ha formulado, el orador propone que el párrafo 2 del proyecto de conclusión 14 diga lo siguiente: 'El hecho de que una controversia se refiera a una norma imperativa de derecho internacional general (ius cogens) es suficiente para establecer, prima facie, la competencia de la Corte [Le fait qu'un différend mette en cause une norme impérative du droit international general (ius cogens, suffit à établir, prima facie, la compétence de la Cour]'. Esta formulación implica que puede establecerse la competencia incluso sin el consentimiento de las partes"[132]

No se tuvieron en cuenta estas propuestas.

Me parece de interés la opinión sobre el tema del juez Bennouna, en su Curso General de La Haya (2016). El internacionalista marroquí valora el distinto alcance de las obligaciones internacionales en atención al interés jurídico que protegen. Estudia, en particular, las obligaciones *erga omnes,* en su concreción por la jurisprudencia del Tribunal Internacional de Justicia[133] y las conecta con el artículo 48 del Proyecto de la Comisión sobre la responsabilidad internacional del Estado, en cuya virtud todo Estado, y no solo el afectado directamente por el hecho ilícito de otro, en los supuestos de violación de este tipo de obligaciones puede exigir, incluso en tu tribunal con jurisdicción en el caso, la responsabilidad del Estado culpable[134].

Y de no poco interés me parece su reflexión, no se percibe que la conclusión 17, párrafo 2, de la Comisión de Derecho Internacional haya movido los sujetos a seguirla en la práctica:

> "Estados, considerados individualmente se mueven por motivos de orden po- lítico, buscando solo la defensa de su propio interés. Y son reticentes a comprometerse en una controversia con otro otros Estados en defensa de un interés colectivo"[135].

B) Ni contramedidas de terceros. El Proyecto de conclusiones de la Comisión (2019) no extiende las consecuencias del *ius cogens* a todos los aspectos del Derecho Internacional de la Responsabilidad.

---

[131] "Capítulo VIII. Normas imperativas de derecho internacional general (i*us cogens*)", *Informe de la de Derecho Internacional. 70º período de sesiones (30 de abril a 1 de junio y 2 de julio a 10 de agosto de 2018). Asamblea General. Documentos Oficiales Septuagésimo tercer período de sesiones Suplemento núm. 10 (A/73/10*), Naciones Unidas, Nueva York, 2018, pp. 244-260, p. 253, párrafo 124

[132] A/CN.4/SR.3420, 4 de julio de 2018, pp. 1-16, p. 4.

[133] Sentencia de 18 de julio de 1966, asunto del Sudoeste africano (Etiopía c . África del Sur; Liberia

c. África del Sur), segunda fase, *International Court of Justice Reports 1966,* pp. 6 ss.; sentencia de 5 de febrero de 1970, Barcelona Traction, Light and Power Company, Limited (Bélgica c . España), *International Court of Justice Reports 1970*, pp. 3 ss.; dictamen consultivo de 8 de julio de 1996, licitud de la utilización de las nucleares por un Estado en un conflicto armado, *International Court of Justice Report 1996*, pp. 66 ss.; dictamen consultivo de 9 de julio de 2004, consecuencias jurídicas de la edificación de un muro en territorio palestino ocupado, *International Court of Justice Reports 2004*, pp. 136 ss.; sentencia de 20 de julio de 2012, cuestiones relativas a la obligación de juzgar o extraditar (Bélgica c . Senegal), *International Court of Justice Reports 2012*, pp. 422 ss.

[134] Sobre el artículo 48 del Proyecto de la Comisión de Derecho Internacional sobre la responsabilidad del Estado por hechos internacionalmente ilícitos y su relevancia recuérdese, ahora, en *vid*. C.Gutiérrez Espada, *La responsabilidad internacional*…, *op. cit.* (nota 72 *supra*), pp. 133-164; ID., "¿*Actio popularis* en Derecho Internacional?", *op . cit.* (nota 91 *supra*), pp. 549-576.

[135] M.Bennouna, *Le Droit International entre la lettre et l'esprit,* The Pocket Books of The Hague Academy of International Law, Brill, M. Nijoff, La Haya, 2017 (es el texto completo del Curso general de Derecho Internacional publico impartido en La Academia de Derecho Internacional de La Haya y publicado en los *Recueil des Cours/Collected Courses,* vol. 383, 2016), pp. 114-115, párrafo 284.

Miembros de la Comisión pidieron que se abordaran al menos ciertas cuestiones, como las que regulaban los artículos 48 (invocación de la responsabilidad por Estados no directamente lesionados) y el artículo 50.1 (contramedidas) de su Proyecto sobre la responsabilidad del Estado por hechos internacionalmente ilícitos de 2001.[136]

El Relator Especial, Sr. Tladi, se oponía al estudio, en el Proyecto de conclusiones, de las contramedidas, cuyo concepto calificaba de controvertido y delicado; mejor (era su opinión) no tratarlo (...)[137]. Y la Comisión la tuvo en cuenta.

A una conclusión similar debió llegar, posiblemente, el juez Bennouna en su Curso General de La Haya (2016), en el que aborda la aplicación forzosa, en su caso, respecto al Estado autor de un hecho ilícito de las consecuencias que el Derecho internacional tiene previstas para quienes incumplen sus mandatos. El profesor Bennouna constata la enorme diferencia que. en cuanto a la aplicación (coercitiva de ser necesario), existe entre el Derecho internacional y los Derechos internos.

Aquel no cuenta con un sistema institucional que pueda, de ser el caso, hacer cumplir las normas; al menos con carácter general. Porque el que existe (y comparto, punto por punto, la reflexión del internacionalista y juez marroquí) no es fiable, por razones de todos conocidos; Mohamed Bennouna indica que el capítulo VII de la Carta otorga al Consejo de Seguridad poderes importantes de naturaleza coercitiva, añadiendo:

> "pero también sabemos que, por su composición, los poderes concedidos a sus miembros permanentes, y el objetivo primario que persigue, el mantenimiento de la paz, este órgano también opera en función de consideraciones de oportunidad política"[138].

En el Derecho internacional vigente, solo las contramedidas pueden servir de herramientas (de autotutela, sin duda) que ayuden a hacer cumplir el Derecho internacional a Estados que espontáneamente se resisten a hacerlo. Lo importante era regularlas con cuidado, a partir de la práctica existente. Y eso ha hecho el Proyecto de la Comisión de Derecho Internacional, cuyas disposiciones en este tema son en conjunto (no comparto la duda de Bennouna) Derecho internacional consuetudinario[139].

Precisamente por esto hubiera sido conveniente que el Proyecto sobre Responsabilidad hubiese concretado más el tema de las contramedidas en dos supuestos concretos:

— Uno, en qué medida podrían jugar para cumplir la obligación que todo Estado tiene que cooperar para poner fin a la violación grave de normas imperativas o acabar con sus consecuencias.
— Y dos, hasta qué punto y con qué límites o condiciones los sujetos no directamente lesionados podrían, en los supuestos previstos por el artículo 54 del Proyecto, adoptar contramedidas contra el culpable.

Y, desde luego, el Proyecto de Conclusiones (2019) no hizo intento alguno de avanzar sobre la situación actual planteada por el artículo 54 del Proyecto de la Comisión de 2001 sobre la responsabilidad del Estado.

Omite, por el contrario, el problema de las eventuales contramedidas de terceros[140]. Que nadie "vió" (...), con la excepción de un miembro de la Comisión, el Sr. Reinish:

---

[136] Entre otros, el Sr. Park (A/CN.4/SR.3416, 1 de junio de 2018, pp. 1-18, p. 17) y la Sra. Galvao Teles (A/CN.4/SR.3419, 3 de julio de 2018, pp. 1-18, p. 4).

[137] C.Gutiérrez Espada,*De la alargada sombra del* ***ius cogens***, op. cit. (nota 129 *supra*), pp. 75-76.

[138] M.Bennouna, *Le Droit International entre la lettre et l'esprit ..., op . cit.* (nota 135 *supra*), p. 135, párrafo 345.

[139] En todo caso, las contramedidas no forman parte en tanto que tales, del derecho internacional consuetudinario pues ello supondría pura y simplemente consagrar la relación de fuerza en la escena internacional" (M.Bennouna, *Le Droit International entre la lettre et l'esprit...*, *op. cit* [nota 135 *supra*], p. 136, párrafo 346). Sobre mi posición respecto de las contramedidas, GUTIÉRREZ ESPADA, C., *La responsabilidad internacional...*, *op. cit*. (nota 72 *supra*), pp. 164-218; ID.: "Función y límites de las represalias (o contramedidas)…", *op. cit.* (nota 74 *supra*), pp. 555-575.

[140] Sobre la importante cuestión, no absolutamente cerrada, de las eventuales contramedida de Estados o de Organizaciones «terceros», esto es, que no resultan directamente lesionados por un Estado u otra Organización internacional que cometen una

> "El problema de las contramedidas no se menciona en el Informe. Una discusión, por ello, y potencialmente una disposición explícita relativa al derecho de terceros Estados a tomar contramedidas contra un Estado que ha violado una obligación con efectos *erga omnes*, podría demostrar ser una adición útil al trabajo de la Comisión. La imposición de contramedidas como una consecuencia de la violación de obligaciones *erga omnes* que, como se ha mencionado supra, incluyen las normas imperativas de derecho internacional general, fue expresamente establecida en la resolución 2005 del Instituto de Derecho Internacional sobre obligaciones *erga omnes* en derecho internacional, el artículo 5 c) de la cual dice: 'si se reconoce ampliamente que una violación grave de una obligación *erga omnes* ocurre, todos los Estados respecto de los que la obligación se debe (...) están habilitados a tomar contramedidas no coercitivas (*non- forcible*) bajo condiciones análogas a aquéllas que se aplican a un Estado especialmente afectado por la violación"[141]

Yo mismo he defendido, en su momento, algo muy parecido[142]. Y, aún aceptando lo delicado de la cuestión y la necesidad de insistir en la adopción de todas las cautelas posibles, no diría la verdad si afirmo, ahora, que ya no lo pienso así. Para este autor al menos, la posibilidad de contramedidas de terceros, con todos los requisitos exigibles, para forzar a quien no quiere a cumplir su deber con el Estado lesionado o las víctimas de la obligación violada, también hubiera sido una muestra de coraje.

Se que esta opinión no es compartida por todos; por doctrina, incluso, que respeto y admiro[143]. Y, sin embargo (...). Qué salida cabe cuando el Sistema, ante hechos terribles, no reacciona (...). Esa misma doctrina que citaba, admite que el recurso actual a acciones de autotutela del tipo de la que he comentado tiene que ver con inacciones clamorosas del Consejo de Seguridad[144].

Más aún, y me pregunto, ¿qué son las "sanciones" y las "medidas coercitivas"adoptadas por muchos Estados y alguna Organización internacional (sujetos no lesionados directamente por la violación del Derecho internacional imperativo cometida por Rusia) contra este país por su agresión a Ucrania y por seguir en su territorio?

52. Y para terminar, conviene aclarar un extremo. En la práctica, las "sanciones" o "medidas coercitivas" que un Estado u Organización internacional víctima de un ciberataque adopta contra los autores del mismo no tienen por qué implicar la adopción de contramedidas contra un Estado. Significativo es el caso de las que decidió imponer la Unión Europea y he comentado *supra*; al adoptarlas, la misma Unión aclara que su decisión no debe interpretarse en el sentido de que considera los ciberataques sufridos imputables a un Estado concreto[145].

---

violación grave de normas imperativas *vid*. RUEDA FERNÁNDEZ, C., "La regulación jurídica de las violaciones graves de obligaciones esenciales emanadas de normas imperativas...", *op . cit*. (*supra* nota 129), pp. 111-115, 115-121; GUTIÉRREZ ESPADA, C., "*¿Quo vadis* Responsabilidad? (Del 'crimen internacional' a la 'violación grave de las normas imperativas')", *Cursos Euromediterraneos Bancaja de Derecho Internacional* (CEBDI), vol. V (2001), pp. 383-564, pp. 523 ss., 540 ss.; ID., "Las contramedidas de Estados 'terceros'", *op . cit.* (nota 91 *supra*), pp. 15-49; ID., *La responsabilidad internacional…, op. cit*. (nota 72 *supra*), pp. 198-205; ID., "La aplicación o ejecución forzosa del Derecho Internacional". *op. cit*. (nota 74 *supra*), pp. 585-595; ID., *La responsabilidad internacional de las organizaciones internacionales a la luz del proyecto definitivo de artículos de la Comisión de Derecho Internacional (2011),* Comares, Granada, 2011, pp. 196-206; ID, "Función y límites de las represalias (o contramedidas) en el Derecho Internacional contemporáneo", *op. cit*., (nota 74 *supra*), pp. 569-575.

[141] A/CN.4/SR.3419, 3 de julio de 2018, pp. 1-18, p. 18.

[142] *Vid. supra* las obras que cito en la nota 140 *supra*.

[143] Así, el artículo 54 del proyecto de la Comisión sobre responsabilidad del Estado, como hemos visto, no considera formada regla alguna que legitime las contramedidas de terceros, pero deja abierta la puerta a ulteriores desarrollos a que pueda llevar la evolución del Derecho Internacional. Incluso cautelas de este tipo preocupan a ese sector doctrinal al que me referido. Ha escrito así recientemente Paz Andrés: "pues supone volver a una práctica mantenida en los años 80 del siglo XX por Estados Unidos y algunos Estados occidentales en casos como el asunto de los rehenes americanos en Irán, la intervención de la URSS en Afganistán o la guerra de las Malvinas, que se consideraba superada y cuya conformidad con el Derecho Internacional era francamente dudosa. En la actualidad, la tardanza del Consejo de Seguridad en adoptar medidas en algunos casos de violaciones graves de los derechos humanos ha vuelto a alimentar esta práctica, como ha , como ha sucedido con la crisis abierta en Siria desde marzo de 2011, en la que los Estados Unidos y la Unión Europea adoptaron medidas contra ese Estado antes de que lo hiciera el Consejo" (P.Andrés Sáenz de Santamaría, *Sistema de Derecho Internacional Público*, Civitas-Thomson Reuters, Editorial Aranzadi, Cizur Menor (Navarra), 2020, 6ª ed., pp. 313-314).

[144] *Vid. supra* nota anterior.

[145] *Vid. supra* párrafo 39 y notas 69 y 70.

Para que un Estado pueda adoptar acciones (cibernéticas o no) contra otro, que respondan a la figura de las contramedidas según el Derecho internacional, debe haber sufrido un ciberataque que pueda imputarse a un Estado o, eventualmente, otro sujeto de Derecho internacional, en aplicación de las reglas sobre imputación o atribución de los hechos ilícitos según el Derecho Internacional de la Responsabilidad y, además, que ese ciberataque implique la violación de una norma internacional en vigor para el autor del mismo. Permítaseme recordar, de nuevo, la Declaración de Nueva Zelanda de 1 de diciembre de 2020:

> "Regardless of whether the activity amounts to an internationally wrongful act, a State may always attribute *political* responsibility for malicious state cyber activity and may always respond with retorsion (i.e. unfriendly acts not inconsistent with international law).
>
> Where a State is subject to cyber activity that amounts to an internationally wrongful act, it may also invoke the international *legal* responsibility of the responsible state. States are responsible for internationally wrongful acts that can be attributed to them, including wrongful cyber activities. An internationally wrongful act can be attributed to a State if it was carried out by organs of the States, persons or entities empowered to exercise elements of governmental authority on behalf of that State, or agents acting on the instructions of, or under the direction or control of the State; or where the State acknowledges and adopts the act as its own. States may also be internationally responsible for aiding or assisting internationally wrongful cyber activity carried out by another State"[146].

[146] NEW ZEALAND, Foreign Affairs and Trade, Crown Law, *The application to International Law to State activity in Cyberspace*, *op. cit*. (nota 109 *supra*), apartados 18-19.