CAPÍTULO II

BLOCKCHAIN Y SEGURIDAD NACIONAL

Vicente MORET MILLÁS
Letrado de las Cortes Generales (Comisión de Defensa, Congreso de los Diputados)
Of Counsel en Andersen
Ignacio SÁNCHEZ GIL
Abogado en Andersen
Doctorando en Derecho Mercantil, Universidad Complutense de Madrid

1. LA TECNOLOGÍA BLOCKCHAIN COMO CONTRIBUCIÓN A LA CIBERSEGURIDAD

La acelerada transformación digital que vivimos se asienta sobre el surgimiento de nuevas tecnologías que se insertan en nuestras vidas de forma disruptiva y a gran velocidad. Las cadenas de bloques representan una de esas tecnologías que, a pesar de haberse desarrollado de forma relativamente reciente, han provocado un notable impacto económico y social. Blockchain es la tecnología de registro distribuido («*distributed ledger technology*») más conocida. Las cadenas de bloques operan mediante un registro que contiene un histórico de información. Este registro, no obstante, no opera de forma centralizada; al contrario, múltiples copias de la misma información se almacenan en registros descentralizados (los llamados «nodos»). Los registros, una vez almacenados, no pueden ser manipulados por uno solo de los nodos sin dejar rastro. Esta es una diferencia esencial con respecto a las bases de datos tradicionales, gestionadas por un operador central que actúa como depositario de la confianza del sistema en su conjunto. Así, la naturaleza descentralizada del mantenimiento de registros proporciona a los usuarios confianza, trazabilidad y seguridad para intercambiar sus datos y/o activos. Existe un gran potencial para el uso de blockchains en múltiples industrias, tales como la de los servicios financieros, las cadenas de suministro, la energía, la sanidad y el sector público.

La tecnología blockchain se está convirtiendo en una suerte de elemento disruptivo en el ámbito digital a tenor de las grandes expectativas que está generando. Si bien es cierto que su impacto real resulta especialmente evidente en la aparición de las criptodivisas, las utilidades y aplicaciones que ya se están desarrollando y se desarrollarán en el futuro trascienden cualquier uso particular, y hacen que esta tecnología esté llamada a tener un impacto real en cuestiones relacionadas con la seguridad nacional de los Estados. El carácter transversal que el ciberespacio tiene en los distintos ámbitos definidos normativamente como actuación en materia de seguridad nacional

supone *de facto* que cualquier cambio tecnológico en el entorno digital vaya a tener consecuencias directas y relevantes en todos los ámbitos en los que se ha divido la acción de los Estados en el cumplimiento de las políticas de seguridad nacional. En este sentido, se puede afirmar que la tecnología blockchain cumple a la perfección con los denominados tres requisitos de seguridad de la información referidos como CIA por sus siglas en inglés: Confidencialidad; Integridad y Disponibilidad («*Confidentiality*», «*Integrity*», «*Availability*»)[1], sin perjuicio de otras consideraciones sobre vulnerabilidades que se desarrollarán más adelante.

La tecnología blockchain posee el potencial para afectar a la seguridad nacional de varias maneras. En este sentido, algunos de estos posibles impactos son:

- Mayor integridad y seguridad de los datos: la naturaleza descentralizada y resistente a la manipulación de las blockchains puede contribuir a garantizar que los datos permanezcan inalterados y seguros. Esto puede ser relevante para las operaciones militares, el intercambio de inteligencia y, en general, a las comunicaciones seguras.
- Seguridad de la cadena de suministro: esta tecnología puede ayudar a detectar y prevenir productos falsificados, garantizar la autenticidad de suministros críticos y mejorar la seguridad general de la cadena de suministro.
- Gestión de la identidad: al aprovechar las técnicas criptográficas de blockchain, los individuos pueden tener un mayor control sobre sus datos personales, reduciendo el riesgo de robo de identidad y fraude. En este sentido, las cadenas de bloques pueden mejorar la seguridad fronteriza, impedir el acceso no autorizado a instalaciones sensibles y mejorar el proceso de investigación de antecedentes del personal.
- Elecciones seguras: Al proporcionar un registro descentralizado e inmutable, blockchain puede evitar la manipulación de los registros de votación, garantizar resultados justos y precisos y aumentar la confianza pública en el proceso electoral.
- Colaboración internacional: La tecnología blockchain puede facilitar la colaboración segura y basada en la confianza entre naciones. Esto puede fomentar la cooperación internacional en ámbitos como el intercambio de inteligencia, la lucha contra el terrorismo y la seguridad fronteriza.

(1) En los términos recogidos en la norma ISO 27001 que establece normas para la seguridad de la información.

1.1. Blockchain como habilitador de la ciberseguridad de sistemas y redes

Aspectos fundamentales para la ciberseguridad tales como la autenticación, la autorización y la auditoría, son potenciados por la tecnología de bloques de forma sustancial en comparación con otros sistemas anteriores. Mejoran las ciberdefensas de los sistemas al asegurar las plataformas e impedir las actividades fraudulentas mediante mecanismos consensuados con un enorme número de actores que dificulta enormemente las actividades dañinas o que permite detectarlas con facilidad, basándose en sus caracteres de inmutabilidad, transparencia, auditabilidad, encriptación y resiliencia operacional. La adopción de la tecnología de cadena de bloques ofrece el potencial para aportar varias ventajas competitivas significativas: permite reducir costes, mejorar la gestión del riesgo y simplificar el cumplimiento normativo de la amplia gama de regulaciones que deben cumplirse y que pueden automatizarse[2].

Según venimos exponiendo, la mayor aportación de esta tecnología frente al *statu quo* es la garantía de la integridad de la información y su trazabilidad, proporcionando a los usuarios una gran certeza sobre la información almacenada. Su estructura descentralizada dificulta enormemente la manipulación de la información, ya que, para que una transacción se añada a la plataforma, la mayoría de los nodos deben estar de acuerdo en que la transacción es válida. Por otro lado, la tecnología blockchain permite una seguridad mucho mayor que los sistemas actuales, demostrando ser extremadamente resistente frente a los ataques DDoS (o ataques de denegación de servicio distribuido, por sus siglas en inglés). Como las blockchains funcionan a través de redes distribuidas, son mucho más complicadas de sobrecargar que las arquitecturas tradicionales, que pueden sufrir interrupciones con mayor facilidad. Cuanto más distribuida esté la red, mayor será el consenso necesario para alterar la información y, por tanto, mayor la protección de la misma.

Sin embargo, blockchain no es una panacea en lo que respecta a la seguridad. No sustituye a otras tecnologías ya desarrolladas y necesarias, sino que complementa los sistemas y protocolos existentes. Así, la confidencialidad sólo puede garantizarse en una red blockchain si la información se cifra a su paso por la red y si también se proponen soluciones válidas para el control de acceso en las redes privadas de blockchain. Una blockchain, por sí misma, tampoco garantiza la exactitud de los datos. Mientras que la estructura distribuida puede asegurar la integridad de los datos alojados una vez introdu-

(2) ENISA. *Tecnología de libro mayor distribuido y ciberseguridad*. Dic. 2016. p. 6.

cidos en el sistema, nada en las cadenas de bloques puede verificar si esa información es correcta (acorde con la realidad fáctica) o no.

Además, no todas las cadenas de bloques son igualmente seguras. Las grandes blockchains —es decir, aquellas cuya información está alojada a través de un gran número de nodos— son menos vulnerables a los ataques, ya que los actores maliciosos necesitarían apoderarse de un número considerable de sistemas distintos para modificar la información alojada. Por el contrario, y como se explica en el Capítulo introductorio de esta obra relativo a las cuestiones estrictamente tecnológicas, las cadenas de bloques más pequeñas (o en fase inicial de desarrollo) pueden correr un mayor riesgo de sufrir un «ataque del 51%», ya que el número de nodos que necesitan ser controlados por los atacantes es sustancialmente menor.

1.2. Aplicaciones y perspectivas geopolíticas

Las posibilidades que abre la tecnología blockchain permiten que algunos países ya la empleen en aplicaciones para las cuales la seguridad es esencial. Así, por ejemplo, Estonia protege los registros de sanidad sus ciudadanos mediante una blockchain específica desarrollada a tan fin; un grupo de bancos japoneses está desarrollando un sistema de pagos móviles instantáneo basado en *Ripple*[3]; los Países Bajos están desarrollando un sistema de control de fronteras que opera mediante tecnología blockchain; IBM y Walmart han puesto en marcha una plataforma para el control de la seguridad alimentaria construida sobre esta tecnología[4]. En definitiva, múltiples iniciativas adicionales están utilizando esta tecnología para desarrollar sistemas que proporcionen una mayor seguridad.

Blockchain, como cualquier otra tecnología, no es intrínsecamente beneficiosa o perniciosa; al contrario, sus efectos positivos o negativos dependerán de la intención de sus usuarios. Si bien son innumerables las iniciativas basadas en blockchains que pretenden aportar beneficios sociales, no puede negarse que este tipo de tecnología distribuida también se ha utilizado para promover agendas de actores malintencionados. Como se verá más adelante, Corea del Norte ha utilizado la tecnología blockchain de diversas maneras

(3) COINTELEGRAPH. *MoneyTap, basado en Ripple, adoptado por tres bancos japoneses*. Abr. 2023. https://cointelegraph.com/news/ripple-based-moneytap-adopted-by-three-japanese-banks

(4) ERICSSON. *Ericsson estima en 31 billones de dólares el mercado de consumo 5G para 2030*. Nov. 2017. https://www.ericsson.com/en/press-releases/2020/11/ericsson-estimates-usd-31-trillion-5g- consumer-market-by-2030

por ejemplo, blanqueando fondos procedentes de fuentes ilícitas o atacando plataformas de intercambio de criptodivisas, o para financiar sus programas de producción de armas de destrucción masiva).

Otra muestra de lo relevante que puede ser la cuestión se refleja en el interés que algunos países están mostrando hacia esta tecnología. Rusia por ejemplo, la considera parte esencial de sus futuros desarrollos en ciberseguridad[5], como se deduce del papel tan relevante que la delegación rusa, formada en parte por antiguos agentes del FSB (Servicio de Inteligencia ruso)[6], tiene en las reuniones de la ISO (*International Standards Organization*) para establecer los estándares internacionales de blockchain. Durante los últimos años, Rusia ha estado tratando de establecer sus algoritmos criptográficos como el principal referente a nivel internacional, con el fin de lograr una ventaja digital, pero también comercial y geopolítica, como ejemplo de lo que se ha denominado *Sharp Power*[7]. Los esfuerzos rusos, sin embargo, se han visto parcialmente frustrados, por un lado, por la existencia de vulnerabilidades (supuestamente intencionadas) en sus algoritmos[8]; por otro, debido a las importantes barreras regulatorias a las que se enfrentan los desarrolladores rusos, lo que les sitúa en una posición de desventaja competitiva frente a soluciones alternativas, como los Estándares Avanzados de Cifrado establecidos por el Instituto Nacional de Estándares y Tecnología de Estados Unidos[9].

2. EL CONTEXTO DE LA SEGURIDAD NACIONAL: LA CIBERSEGURIDAD COMO ESTRATEGIA

La seguridad, en cualquiera de sus dimensiones, es la responsabilidad primordial de un Estado. Históricamente, el mantenimiento de la seguridad de un país o sociedad ha sido un deber asumido por las fuerzas públicas para mantener el orden interno, y empleando medios militares. Sin embargo, la aparición de nuevos actores y riesgos de naturaleza heterogénea ha llevado a muchos Estados a llevar a cabo una profunda revisión y transformación de

5) WALL STREET JOURNAL. La criptodivisa puede promover la seguridad nacional. Dic. 2017. https://www.wsj.com/articles/cryptocurrency-can-promote-national-security-1513280417

6) NEW YORK TIMES, *Blockchain será suyo, se jactó el espía ruso en una conferencia*. Abr. 2018. https://www.nytimes.com/2018/04/29/technology/Blockchain-iso-russian-spies.html

7) ASUNTOS EXTERIORES, extraído de https://www.foreignaffairs.com/articles/china/2017-11-16/meaning-sharp-power

8) VICE. *Experts Doubt Russian Claims That Cryptographic Flaw Was a Coincidence*. May. 2019. https://www.vice.com/en/article/43j3wm/experts-doubt-russian-encryption-standard-cryptography- backdoor-streebog-kuznyechik

9) FINTECHRU. El *FSB ruso complica la vida a las empresas Blockchain*. Julio de 2020. https://www.fintechru.org/publications/russia-s-fsb-is-making-life-harder-for-Blockchain-companies/

sus políticas de seguridad y defensa. En otras palabras, los Estados conservarán sin duda su función más primordial: proporcionar seguridad a sus ciudadanos; sin embargo, lo harán de una forma diferente, más integrada, coherente y polivalente: utilizando todas las capacidades públicas para hacer frente a nuevas amenazas que son ahora más híbridas, líquidas y difusas. En la mayoría de los casos, estas nuevas amenazas tienen un fuerte componente cibernético, ya sea como medio indispensable de agresión o como objetivo en sí mismo. A este nuevo marco conceptual integrado se le denomina seguridad nacional entendida como una política gubernamental de carácter global.

2.1. Ciberespacio, Estados y Derecho

La seguridad no era una de las principales preocupaciones de los creadores de la internet. Esto se pospuso para promover otros aspectos del desarrollo digital y puede decirse que el ciberespacio y el derecho eran dos realidades paralelas. Así se concibió la red, como una especie de paradigma de anarquía perfecta sin reglas y sin Estados. Mientras operaba bajo esta estructura alegal, el impacto de la propagación de las TIC ha sacudido todas y cada una de las esferas de nuestra vida social, económica e incluso política. Esta nueva normalidad estaba fuera y por encima de la acción soberana del Estado y de sus herramientas y leyes.

Poco a poco, los Estados europeos y la Unión Europea han ido intentando regular mediante el Derecho, tanto a nivel nacional como internacional, un espacio que estaba vacío de intervención pública. Se cumple así una realidad inmutable: *ubi societas ibi lex*. Donde hay un vacío, las sociedades humanas tienden a llenarlo con la fuerza de la ley o con la ley de la fuerza. Como expresión de esta última necesidad, puede decirse que el Derecho internacional debe «civilizar» estas nuevas amenazas internacionales a la paz y a la estabilidad mundial creadas por los nuevos medios de confrontación y conflicto en el ciberespacio. Sin embargo, las dificultades para lograr esta necesaria regulación son muchas. Desde el punto de vista de la seguridad nacional, el elemento clave que define y limita la acción de los Estados es la soberanía nacional, fundamento del orden internacional postwestfaliano. La soberanía se estructura necesariamente sobre un elemento corpóreo, en la medida en que se ejerce sobre una parte de la superficie terrestre y, como tal, encuentra obstáculos en el ciberespacio, un lugar sin territorio. Internet se concibió como un espacio virtual sin límites ni fronteras, un nuevo escenario para la acción humana abierto y no sujeto a ninguna soberanía. Si bien

es cierto que algunos países con regímenes autoritarios, como China, han amurallado ese ámbito digital, la apertura y la libertad siguen siendo la característica fundamental que predomina en el ciberespacio.

2.2. Nuevas amenazas para la seguridad nacional

Por otra parte, la seguridad de los Estados ya no está restringida a la defensa de sus fronteras y su soberanía, sino que también debe garantizar el bienestar de sus sociedades frente a nuevos y diversos riesgos. La globalización y la aplicación masiva de las tecnologías de la información fomentan la aparición de nuevos riesgos y amenazas transfronterizos como el terrorismo internacional, el ciberterrorismo o los ciberataques contra infraestructuras críticas. La aparición de actores con orígenes y motivaciones heterogéneas con la voluntad de desafiar el Estado de Derecho, los ordenamientos jurídicos y el Orden Internacional, e incluso con la intención de imponer sus formas de entender el mundo o la vida es una realidad que se ha manifestado ya de forma evidente. El ciberespacio ha proporcionado la capacidad para actuar en cualquiera de las dimensiones de la seguridad, disminuyendo las posibilidades de respuesta de los Estados agredidos. En definitiva, un nuevo reto se plantea ahora en todos los sistemas cuyos gobiernos tienen la obligación constitucional de velar por la vida y seguridad de sus ciudadanos, atribuida como el principal de los fines del Estado desde que este nace, tal y como hoy lo conocemos, en los albores del Siglo XV.

Este reto no es otro que afrontar con resolución una nueva tarea de vital importancia en los Estados actuales asegurando la libertad de los ciudadanos con su seguridad y la realización del Derecho[10]. Al conseguirlo, se logrará una inmensa ventaja competitiva frente a otras naciones. Por lo tanto, los Estados democráticos necesitan ciberseguridad al tiempo que garantizan el respeto de los derechos y libertades[11]. De lo contrario, las amenazas procedentes del ciberespacio pueden cambiar nuestro modo de vida, lo que es intolerable desde el punto de vista de un Estado demo-liberal. No se puede aceptar que un elemento ajeno a la soberanía nacional sea capaz de impedir que una determinada comunidad política se desarrolle libremente.

La irrupción del ciberespacio como nuevo dominio implica un cambio civilizatorio con innumerables consecuencias. Sólo en el período de 2015 a 2020, la proporción de usuarios de Internet en el mundo pasó del 40% al

(10) KELSEN, H., Teoría General del Estado. Editorial Nacional, México, 1979. Página 55.
(11) GARCÍA MEXÍA, P., *El Derecho de Internet*, Atelier libros jurídicos, 2016. Página 23.

60% de la población mundial[12]. Si añadimos la capacidad de causar graves daños a las infraestructuras críticas de un Estado, o a sus sistemas financieros, así como la perspectiva de influir en los sistemas políticos, la relevancia del ciberespacio en relación con la seguridad de los Estados es evidente. En este nuevo escenario, algunos elementos son clave desde el punto de vista de la seguridad nacional, como el fin de los límites espaciales y temporales, como categorías centrales en el funcionamiento de los Estados. La globalidad, el anonimato, la omnipresencia digital, el multilateralismo, la infoxicación y el cambio constante caracterizan la nueva normalidad. Internet no es un espacio físico; sin embargo, es un espacio real y por eso los Estados reaccionan estando presentes en la red. A veces cumpliendo la ley; a veces sin normas que regulen su actuación. Por este motivo, los Estados y el ciberespacio mantienen una relación extremadamente compleja y divergente desde la aparición de este último.

Por tanto, esta es la primera dificultad a la hora de regular hipotéticos peligros emanados de la red, ya que la actuación de los Estados y, por tanto, la aplicación del poder público y de las normas se limita al ámbito territorial de la soberanía: las fronteras geográficas. Se dice con razón que: «*(l)os reguladores siguen intentando gestionar esta máquina con reglas concebidas para la era industrial*»[13].

El segundo reto al que se enfrentan los Estados para combatir las diversas amenazas que emanan de la red tiene que ver con la dificultad de identificar a los autores que están detrás de las amenazas, lo que limita la actuación de los poderes públicos frente a enemigos cuya identidad y origen permanecen desconocidos. De hecho, en el ámbito militar se ha conceptualizado un nuevo tipo de conflicto bélico, las guerras de 4ª Generación[14], o guerras híbridas, en las que el uso de las tecnologías de la información y la comunicación es determinante. Este entorno posibilita estrategias asimétricas, de tal forma que un grupo o país con escasas capacidades militares puede suponer una amenaza compleja para un Estado con mayores recursos. La ubicuidad de estas tecnologías y la relativa imposibilidad de rastrear los ataques hacen que la disuasión no sea tan eficaz en este ámbito de la seguridad y la defensa como en otros. La disuasión es la piedra angular en la que se basa

(12) Obtenido de https://data.worldbank.org/indicator/IT.NET.USER.ZS
(13) TAPSCOTT, D., *Revolución Blockchain*, 2016. Página 56.
(14) KALDOR, M., *Las nuevas guerras*, Tusquets, Madrid, 2001. Página 15.

la defensa, y supone la renuncia a atacar por el posible daño que se pueda recibir[15].

La seguridad total en el ciberespacio es difícil de alcanzar porque, como hemos comentado, la arquitectura de Internet fue diseñada para promover la conectividad, no la seguridad[16]. Las ciberamenazas, por sus características, cuestionan incluso un principio esencial del actual orden geopolítico vigente desde la Paz de Westfalia, que no es otro que el del protagonismo de los Estados como ejes en torno a los cuales se desarrolla la geopolítica mundial. Por ello, la ciberseguridad en los países se formula, desarrolla e implementa cada vez más como una especialidad más dentro del esquema general de la seguridad de los Estados, concibiéndose como una política de Estado decisiva para garantizar la prosperidad y la estabilidad.

2.3. Ciberseguridad nacional frente a amenaza global

En este sentido, la información en tiempo real, que permite visualizar lo que está ocurriendo en cualquier lugar del Globo, sensibiliza a la opinión pública sobre la violencia y los conflictos, creando percepciones que afectan significativamente a las decisiones de los poderes públicos. En algunos casos, esto puede contribuir a la caída de gobiernos, como se vio en la primavera árabe o, pocos años después, en Ucrania, entre otros. En este nuevo contexto, se produce una transnacionalización de los conflictos internos, confundiendo seguridad interior y exterior. Podemos decir que el ciberespacio vive en un estado de agresión permanente en el que todos los usuarios, sean del tipo que sean, pueden ser objetivos, independientemente de su grado de protección[17]. El uso de estas tecnologías como armas recupera la afirmación clausewitziana de que los conflictos no son de naturaleza militar sino política y están directamente relacionados con la lucha por el poder político, ya que su objetivo principal no es otro que el de debilitar un Estado socavando su legitimidad. Además, el ciberespacio ofrece a los grupos terroristas medios de propaganda, comunicación, financiación y reclutamiento. También las organizaciones criminales buscan y consiguen llevar a cabo *ransomware*, robos o acciones de robo de información o ciberespionaje.

(15) FELIU ORTEGA, L., «La ciberseguridad y la ciberdefensa», *Monografías del CESEDEN*, NÚM. 126, Ministerio de Defensa, 2011. p. 41.
(16) THE ECONOMIST, Defender la frontera digital, 12 de julio de 2014.
(17) GÓMEZ DE ÁGREDA, A., «El ciberespacio como escenario de conflicto. Identificación de amenazas», *Monografías CESEDEN*, nº 126, Ministerio de Defensa, 2011. p. 180.

Por ello, la naturaleza de las amenazas es multiforme, y por eso los mecanismos de reacción de cada Estado deben basarse en los principios de unidad de acción (imprescindible para poder hacer frente con garantías de éxito), y de compartición de capacidades.

2.4. Cuantificando el reto

Las amenazas son múltiples y bien conocidas, pero merece la pena recordar algunas de ellas para subrayar la relevancia que los planes de ciberseguridad tendrán para la supervivencia de un país ahora y en el futuro. Entre 2007 y 2008, Rusia dirigió una serie de ciberataques ofensivos contra Estonia y Georgia, provocando daños materiales significativos. Esto, sin embargo, parece una anticipación de lo que ocurriría años más tarde, cuando el Kremlin llevó a cabo campañas sistemáticas de ciberataques contra objetivos públicos y privados ucranianos, como forma de complementar las hostilidades que tenían lugar en el dominio físico. Otros ejemplos destacables de los últimos años podrían ser el ataque *NotPetya* de 2017, que provocó más de 10.000 millones de dólares en daños a nivel global, y está considerado como el ciberataque más costoso de la historia[18]; o el *ransomware* que en 2018 infectó Colonial Pipeline, la entidad que gestiona la mayor red de oleoductos de Estados Unidos, provocando desabastecimiento en gran parte del país y, en último término, motivando que el presidente Biden declarase el estado de emergencia[19].

Cada día es mayor el número de incidentes graves de ciberseguridad que son conocidos públicamente. Se trata de una característica que define el propio contexto; es una amenaza permanente, cambiante y creciente. Los datos lo demuestran. Según el Informe Anual de Seguridad Nacional de España de 2021, la cantidad total de incidentes disminuyó ligeramente de 82.530 en 2020 a 69.202 en 2021. Esta cifra, sin embargo, sigue siendo relativamente alta si se compara con los 42.995 incidentes que se produjeron en 2019. Los incidentes considerados críticos, sin embargo, aumentaron de 62, en 2020, a 139 en 2021[20]. Dentro de las infraestructuras críticas, los sectores

(18) WIRED. La historia no contada de NotPetya, el ciberataque más devastador de la historia. Agosto de 2022. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

(19) BBC. Los piratas informáticos del oleoducto estadounidense «no pretendían crear problemas». Mayo 2021. https://www.bbc.com/news/business-57050690

(20) DEPARTAMENTO DE SEGURIDAD NACIONAL, Informe Anual de Seguridad Nacional 2021. P43. https://www.dsn.gob.es/es/documento/informe-anual-seguridad-nacional-2021

más afectados fueron la administración pública (32%), el transporte (29%) y el sector financiero (23%)[21].

Según Norton[22], más de 415 millones de consumidores en todo el mundo fueron víctimas de alguna forma de ciberdelincuencia en 2022. McAfee y el Centro de Estudios Estratégicos e Internacionales afirman que, en 2020, el coste global de la ciberdelincuencia representó el 0,8% del PIB mundial (600.000 millones de dólares).

Sin perjuicio de que las anteriores estadísticas evidencian una tendencia innegable, no debe perderse de vista que estas u otras cifras proporcionadas por empresas de seguridad informática deben interpretarse siempre con cautela por la falta de métodos de cuantificación totalmente fiables.

2.5. Los atacantes y sus objetivos

Las amenazas provenientes del ciberespacio provienen de fuentes heterogéneas, pudiendo sistematizarse de la forma siguiente:

Individuos aislados, que, dadas las características asimétricas del escenario, pueden cometer delitos o causar daños graves.

Hacktivistas, que persiguen el control de redes o sistemas para promover sus objetivos o defender sus posiciones políticas o sociales, atacando sitios web, robando y publicando datos sensibles, o llevando a cabo otras acciones disruptivas. En el contexto de la invasión rusa de Ucrania, hemos sido testigos de la importancia que pueden tener este tipo de grupos relativamente desestructurados, con el ejemplo del llamado «Ejército IT de Ucrania», un conglomerado de individuos, organizaciones y representantes del gobierno ucraniano que se coordinan a través de foros privados, Twitter y Telegram, principalmente. Este Ejército IT ha llevado a cabo una serie de ciberataques contra infraestructuras rusas, como la Bolsa de Moscú, o el Ministerio de Transformación Digital, entre muchos otros[23].

(21) Ibid.

(22) NORTON. Informe sobre ciberseguridad. 2022 https://www.nortonlifelock.com/us/en/newsroom/press-kits/2022-norton-cyber-safety-insights-report— special-release-online-creeping/

(23) MICROSOFT. Informe de defensa digital de Microsoft 2022. 2022. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bUvv?culture=en-us4&country=us

Organizaciones criminales, que utilizan la red como medio, objetivo o lugar de comisión de delitos como el fraude telemático, el blanqueo de capitales, el robo de información o el ransomware.

Organizaciones terroristas, que causan el pánico en la población o provocan catástrofes atacando infraestructuras críticas. Estos grupos también encuentran en las actividades ciberhostiles un medio para comunicarse, publicitarse y financiarse.

Organizaciones extremistas, que utilizan la red para difundir sus mensajes.

Ciberespías, o atacantes destinados a obtener secretos de Estado, información relevante de cualquier fuente, ya sea pública o privada, propiedad industrial, información comercial sensible o información personal. Detrás de esta clase de agentes pueden encontrarse servicios de inteligencia, fuerzas armadas o empresas privadas.

Estados extranjeros, a través de organismos estatales, o directamente a través de sus fuerzas armadas o aparatos de seguridad. Tradicionalmente, se ha asumido que, mediante los ciberataques, los estados persiguen objetivos estrictamente políticos (en contraste con los económicos), como la interrupción de la infraestructura de estados rivales para ejercer influencia política, o el acceso a información confidencial. En los últimos años, sin embargo, se ha podido atestiguar cómo Estados soberanos han llevado a cabo ciberataques como forma de financiar su presupuesto. Nos referimos al caso de Corea del Norte: un informe de 2019 elaborado por el Grupo de Expertos del Comité de Sanciones de la República Popular Democrática de Corea (RPDC) de la ONU[24] muestra cómo el país asiático obtuvo unos ingresos totales superiores a los 2.000 millones de dólares a través de ciberataques con ánimo de lucro, que posteriormente fueron utilizados para financiar la producción de armas de destrucción masiva. Es reseñable que la tecnología blockchain desempeñó un papel importante durante todo este proceso: en primer lugar, porque algunas de las principales víctimas de Corea del Norte fueron plataformas de intercambio de criptodivisas[25] (causando pérdidas de hasta 31 millones de dólares); en segundo lugar, porque las criptodivisas se utilizaron para facilitar el blanqueo de dinero y obstaculizar las capacidades de rastreo de las autoridades de otros Estados.

(24) CONSEJO DE SEGURIDAD DE LA ONU Informe S/2019/691. 2019. p. 26. https://www.securitycouncilreport.org/atf/cf/%7b65BFCF9B-6D27-4E9C-8CD3—CF6E4FF96FF9%7d/S_2019_691.pdf

(25) Ibid.

Una de las mejores formas de esclarecer la naturaleza de una amenaza ciberespacial se basa en determinar si dicha amenaza se dirige contra la capa sintáctica, la capa semántica o la capa física del ciberespacio[26]. Así, la capa semántica estaría compuesta por los datos, los programas y, en general, todo el conocimiento acumulado en los servidores y ordenadores. La capa sintáctica estaría formada por los protocolos, sistemas operativos y otros lenguajes utilizados para hacer que los programas funcionen y los datos sean legibles, permite que los sistemas se comuniquen entre sí. Por último, la capa física sería todo lo que podemos ver y tocar en un ordenador: discos duros, monitores, teclados y servidores, líneas de cable o satélites.

Según ENISA —la Agencia de Ciberseguridad de la Unión Europea—, algunos de los sectores más atacados dentro de la UE son el de las administraciones públicas (24,21%), el de los servicios digitales (13,09%), el financiero (8,64%), o el de la salud (7,2%)[27].

2.6. Amenazas híbridas, respuestas híbridas

¿Cómo pueden responder los Estados a este tipo de amenazas? Como hemos mencionado, una de las principales razones por las que los actores maliciosos utilizan el ciberdominio para llevar a cabo sus operaciones es el anonimato estructural que caracteriza a la red. Esto pone en una situación compleja a los Estados, que a menudo se ven incapaces de encontrar pruebas suficientes para atribuir claramente una actividad hostil a un grupo o Estado específico.

Los expertos en disuasión —que puede definirse como la «*prevención de la acción, ya sea por la existencia de una amenaza creíble de contraacción inaceptable y/o la creencia de que el coste de la acción supera los beneficios percibidos*»[28] diferencian entre disuasión activa (la amenaza de represalias) y pasiva (la capacidad de frustrar los ataques). Debido a las dificultades en el proceso de identificación (y, por tanto, de represalia) de los actores maliciosos, los Estados democráticos han centrado la mayor parte de sus esfuerzos en la disuasión pasiva y, como tal, han buscado incrementar sus capacidades de ciberdefensa para desalentar posibles ataques. Esta ha sido la perspectiva de la Unión Europea que, para mejorar su protección contra los actores

(26) LIBICKI, M., Ciberdisuasión y ciberguerra, Rand Corporation, 2009. p. 12.
(27) ENISA. Panorama de amenazas 2022 de ENISA. 2022. p. 15. https://www.enisa.europa.eu/publications/enisa-threat landscape-2022.
(28) McKenzie, Timothy M. ¿Es posible la ciberdisuasión?.2017. p. 14. https://media.defense.gov/2017/Nov/20/2001846608/-1/1/0/CPP_0004_MCKENZIE_CYBER_DETERRENCE.PDF.

malintencionados, ha aprobado recientemente dos importantes actos legislativos: la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) n.º 910/2014 (Directiva NIS 2) y el Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 sobre la resiliencia operativa digital del sector financiero (Reglamento DORA). En conjunto, estas normas obligarán a una serie de actores que operen en sectores esenciales a aplicar medidas para minimizar la probabilidad y el impacto de los ciberataques.

Otros sistemas políticos, sin embargo, han mostrado más interés en la disuasión activa y, por tanto, han reconocido públicamente su intención de contraatacar a los actores maliciosos. La Estrategia de Ciberseguridad de Estados Unidos 2023 reconoce que la interrupción y el desmantelamiento de los actores de amenazas son sus cinco principales líneas de actuación, afirmando que «*Estados Unidos utilizará todos los instrumentos del poder nacional para interrumpir y desmantelar a los actores de amenazas cuyas acciones amenacen nuestros intereses. Estos esfuerzos pueden integrar capacidades diplomáticas (...) militares (...). Nuestro objetivo es hacer que los actores maliciosos sean incapaces de montar campañas cibernéticas sostenidas*».

3. BLOCKCHAIN COMO TECNOLOGÍA CENTRAL DE LAS CRIPTODIVISAS Y SUS IMPLICACIONES PARA LA SEGURIDAD NACIONAL

Como prueba el posterior Capítulo de esta obra dedicado a ese concreto tema, la aparición de las criptodivisas ha supuesto un elemento disruptivo en el panorama financiero mundial. En este sentido, las criptodivisas pueden verse como una magnífica oportunidad para generar y financiar actividad económica y talento al servicio de la humanidad, aunque de las mismas también puedan derivarse amenazas para la seguridad del sistema financiero. Al desafiar la actual supremacía de los gobiernos en la administración del sistema económico y monetario, se desplaza un aparato bien establecido, reglado e intervenido por las instituciones públicas. La tecnología puede ser vista como una amenaza o como una oportunidad para mejorar nuestras sociedades, y esto se aplica, por supuesto, a la tecnología blockchain.

3.1. Criptodivisas y blanqueo de capitales

Las criptodivisas —y las cadenas de bloques en general— se crearon con la intención de desintermediar las relaciones humanas y, más concretamente,

las comerciales. Bitcoin, la primera blockchain, surgió durante la crisis financiera de 2008 como alternativa al sistema monetario y a los amplios poderes de los bancos centrales[29]. Las criptodivisas operan bajo la premisa de que no se requiere de un intermediario (un banco, o un juez) para supervisar o ejecutar («*enforce*») las transacciones. Al contrario, es el propio funcionamiento de blockchain lo que garantiza que las transacciones se lleven a cabo. Una transacción de Bitcoins no necesita de ninguna institución central para ejecutarse; la red blockchain ejecuta la transacción «automáticamente» según su código programado.

Las criptodivisas, por tanto, funcionan sin recurrir a los intermediarios clásicos. La experiencia demuestra que, aunque la tendencia de las blockchains a desintermediar es innegable, no se ha logrado una descentralización total, y la mayoría de las blockchains dependen de ciertas formas de intermediación para funcionar correctamente. Probablemente, uno de los mejores ejemplos sean los proveedores de los conocidos como «monederos calientes» o «*hot wallets*». La mayoría de las blockchains requieren que los usuarios recuerden dos «claves» criptográficas (una pública y otra privada) para operar. Estas claves son secuencias alfanuméricas aleatorias que funcionan como contraseñas. Sin embargo, la dificultad de memorizarlas (las secuencias suelen ser extremadamente largas) hace que muchos usuarios recurran a los *hot wallets*, que son servicios que almacenan las claves criptográficas y ofrecen una interfaz al usuario. Los proveedores de *hot wallets* suelen ser entidades legalmente constituidas que, *de facto*, actúan como intermediarios, aunque de forma diferente a los intermediarios tradicionales, como bancos o *brokers*. Las plataformas de intercambio de criptodivisas son otro caso interesante: estos servicios permiten a los usuarios intercambiar criptodivisas por dinero de curso legal, o por otras criptodivisas.

Es notorio que las criptodivisas se utilizan como refugio para el dinero procedente de actividades ilegales. Según algunas estimaciones, en 2021 se blanquearon 8.600 millones de dólares a través de criptodivisas[30]. La delincuencia y las criptodivisas están relacionadas desde los orígenes de Bitcoin en 2009. De hecho, existen opiniones favorables a la tesis de que Bitcoin nació precisamente como una herramienta de intercambio anónimo para

(29) AIBC. Día del Bloque Génesis: Bitcoin cumple 14 años. Jan. 2023. https://aibc.world/news/genesis— block-day-Bitcoin-turns— 14/#:~:text=%E2%80%9CThe%20Times%2003%2FJan%2F,of%20a%20bank%20bailout%20broke

(30) CHAINANALYSIS. DeFi adquiere mayor protagonismo en el blanqueo de capitales, pero sigue dominando un pequeño grupo de servicios centralizados. Eneo de 2022. https://blog.chainalysis.com/reports/2022-cryto-crime-report-preview-cryptocurrency-money—laundering/

facilitar transacciones ilegales a través de *Silk Road*, el mayor mercado negro online del mundo hasta que fue cerrado por el FBI. Los operadores de la *Deep Web* necesitaban una forma anónima de pagar para poder realizar transacciones y eludir posibles investigaciones de las fuerzas de seguridad.

Existen muchos ejemplos de actividades delictivas que utilizan la criptodivisa como sistema para blanquear fondos obtenidos ilegalmente. Uno de estos usos muy frecuentes son los casos de ransomware en los que se utilizan divisas virtuales como medio de pago. El más notorio de los ciberincidentes de ransomware a escala global fue *WannaCry*, un *ransomware* que infectó a miles de empresas, entre ellas, aunque mínimamente, Telefónica. El virus secuestró y encriptó más de 300.000 equipos informáticos en todo el mundo, exigiendo pagos en Bitcoin para liberarlos. Algunas empresas estiman el coste potencial del ataque en unos 5.000 millones de dólares[31]. *WannaCry* sólo tenía sentido, aparentemente, si los atacantes podían obtener un beneficio económico de la operación, premisa que pudo cumplirse gracias a Bitcoin. El ya referido informe de 2019 del Panel de Expertos de la ONU del Comité de Sanciones de la República Popular Democrática de Corea (RPDC) [32] describió cómo Bitcoin desempeñó un papel crucial para el blanqueo de los rescates de WannaCry:

> *«Los pagos de rescate en Bitcoin realizados por las víctimas de WannaCry se transfirieron desde una cartera de Bitcoin a través de intercambios de criptodivisas y, en última instancia, se convirtieron a Monero, otra criptodivisa, utilizando un intercambio de criptodivisas con sede en Suiza llamado ShapeShift. (...) En agosto de 2018, menos de dos meses después del ataque, los fondos se enviaron a YoBit en una compleja serie de cientos de transacciones con el objetivo de convertir y cobrar la totalidad de la criptodivisa robada».*

Las criptodivisas son muy atractivas para la actividad delictiva por varias razones. La primera y más importante es el anonimato. Algunas criptodivisas son completamente anónimas, como Monero, Zcash o Dash (el primer nombre de Dash fue Dark Cash). Durante los últimos años, el uso de estas criptodivisas anónimas ha crecido significativamente en la *Dark Web*[33]. El resto no son completamente anónimas, sino pseudoanónimas[34], lo que significa que, si se conoce la identidad de alguno de los propietarios de la cartera, es

(31) CONSEJO DE SEGURIDAD DE LA ONU, op. cit. p. 26.
(32) Ibídem, p. 28.
(33) EUROPOL. IOCTA 2021. p. 37. https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assess ment_iocta_2021.pdf
(34) PARLAMENTO EUROPEO, Divisas virtuales. Diálogo monetario julio 2018. Parlamento Europeo. PE 619.016. p. 11.

posible rastrear el hash y exponer su identidad real. Sin embargo, esto lo anterior nos adentraría en el terreno de la especulación, ya que dicha labor requeriría un análisis muy complejo y costoso en cuanto a tiempo y recursos.

El anonimato que caracteriza intrínsecamente al entorno blockchain puede incrementarse «artificialmente» mediante el uso de herramientas, como los mezcladores o «*mixers*». Estas plataformas permiten a diferentes usuarios depositar sus criptodivisas y, a continuación, todas las divisas de los usuarios se «mezclan» entre sí, dificultando la trazabilidad por parte de las autoridades públicas.

La segunda gran ventaja de las divisas virtuales para la actividad delictiva es consecuencia directa de la ausencia de intermediarios sujetos a control regulatorio que caracteriza a la mayoría de las blockchains. Nuestro sistema de regulación financiera se basa en gran medida en la existencia de intermediarios que se encuentran en una posición única para informar y bloquear transacciones sospechosas. Por ejemplo, los bancos desempeñan un papel crucial en la prevención del blanqueo de capitales, por lo que están sujetos obligaciones de «*know your customer*» en virtud de las cuales deben estudiar y controlar a algunos de sus clientes, y el origen de sus fondos, siendo así la primera línea de defensa para combatir el blanqueo de dinero procedente de actividades delictivas.

En el caso de España, la Ley 10/2010, de prevención del blanqueo de capitales y de la financiación del terrorismo, junto con el Real Decreto 304/2014, impone responsabilidad penal a los intermediarios financieros, como bancos o despachos de abogados en caso de contribuir al blanqueo de capitales. También están obligados a informar al SEPBLAC (Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales) de la detección de ciertos indicios de blanqueo de capitales, no pudiendo escudarse en la existencia de secreto profesional para inobservar sus deberes. El incumplimiento de estas normas puede acarrear sanciones relevantes e incluso responsabilidades penales.

Los legisladores intentan adaptarse a las peculiaridades que caracterizan el entorno blockchain. El Real Decreto-Ley 7/2021 transpuso la Directiva 2018/843, y modificó la Ley 10/2010 para establecer obligaciones contra el blanqueo de capitales para los proveedores de servicios de *hot wallets*, y para los intercambios de criptodivisas. Aunque las blockchains tienen carácter transnacional, las autoridades públicas se niegan a permitir que el mercado de las criptodivisas opere de forma autónoma. Para ello, intentan influir en

sus actividades a través de la regulación de determinados «puntos de contacto» (en este caso, *hot wallets* y plataformas de intercambios) que forman parte del ecosistema blockchain, pero que no funcionan de forma descentralizada.

Sin embargo, pensar que la regulación de las *hot wallets* será suficiente para controlar las diferentes amenazas derivadas del entorno blockchain sería ingenuo. Los actores maliciosos suelen recurrir a la denominada «infraestructura gris», es decir, servicios (bolsas de criptodivisas, mezcladores, proveedores de servicios de monedero) establecidos en países con escasa o nula legislación contra el blanqueo de capitales y que evitan la cooperación con las fuerzas de seguridad internacionales[35].

La combinación de anonimato y transacciones financieras descentralizadas puede implicar formidables retos regulatorios. Mientras que, en algunos casos, el acceso a las blockchains estará intermediado por entidades como los proveedores de servicios de *hot wallet* (que no están descentralizados y, por tanto, pueden verse sujetos a regulación), la infraestructura gris ofrece a los actores maliciosos una alternativa válida. La única forma de combatir la infraestructura gris con garantías de éxito sería hacerlo desde un nivel supranacional. En marzo de 2023, el FBI anunció el desmantelamiento de ChipMixer, una de las mayores plataformas de mezclas que era utilizada sistemáticamente por delincuentes, Estados como Corea del Norte, y otros actores maliciosos. Para llevar a cabo su investigación, las autoridades estadounidenses tuvieron que colaborar con la EUROPOL, la policía cibernética polaca y la policía estatal de Zúrich[36]. De forma similar, y sólo un mes después, el FBI y la Policía Nacional de Ucrania informaron de la interrupción de las operaciones de nueve servicios de intercambio de criptodivisas que incumplían sistemáticamente la legislación contra el blanqueo de capitales y servían «como importantes centros del ecosistema de la ciberdelincuencia»[37]. Como demuestran estos ejemplos, las amenazas descentralizadas y ubicuas sólo pueden ser gestionadas eficazmente por la comunidad internacional, actuando de forma coordinada.

(35) EUROPOL. Op. cit. p. 38.

(36) DOJ. Justice Department Investigation Leads to Takedown of Darknet Cryptocurrency Mixer that Processed Over $3 Billion of Unlawful Transactions. Marzo de 2023. https://www.justice.gov/opa/pr/justice-department-investigation-leads-takedown-darknet-cryptocurrency— mixer-processed-over-3

(37) DOJ. El FBI desbarata intercambios de divisa virtual utilizados para facilitar actividades delictivas. Abr. 2023. https://www.justice.gov/usao-edmi/pr/fbi-disrupts-virtual-currency-exchanges— used-facilitate-criminal-activity

3.2. Las criptodivisas como riesgo potencial para la seguridad económica y financiera

Aunque Bitcoin fue la primera criptodivisa desarrollada, la capitalización total del mercado de los criptoactivos a finales de diciembre de 2022 rondaba los 840.490.000.000 dólares[38]. El valor de mercado de Bitcoin (596.504.607.566 dólares) constituye la mayor parte de la capitalización de mercado total hasta ahora. Otros activos importantes son Ether (253.589.192.319 $) y Tether (80.837.843.577 $). A lo largo de los años, el crecimiento de las criptodivisas ha sido exponencial. En este sentido, debe recordarse que, en el primer trimestre de 2017, su valor de mercado acumulado no superaba los 30.000 millones de dólares[39].

Es dudoso que criptodivisas como Bitcoin o Ether puedan sustituir al dinero *fiat* a corto plazo (debido a la alta volatilidad de sus precios provocada por la especulación financiera). Sin embargo, en los últimos han surgido iniciativas que pretenden solucionar el problema de los cambios bruscos de precio: son las *stablecoins*, criptodivisas que recurren a medidas como la gestión algorítmica de la oferta monetaria, o la custodia de depósitos, para mantener un precio estable. USD Coin, por ejemplo, es una stablecoin cuyo valor está vinculado al dólar estadounidense. Si este tipo de activos logran una relativa estabilidad de precios, pueden constituir una amenaza para los poderes de los bancos centrales y, por ende, para todo el sistema monetario actual.

Otros criptoactivos constituyen una alternativa al actual funcionamiento del sistema financiero (no monetario). Las ICOs (*Initial Coin Offerings*) son procesos organizados a través de los cuales un emisor ofrece criptoactivos al público, a cambio de financiación. Estos activos normalmente otorgan ciertos derechos económicos a su propietario, como una acción, un bono u otros instrumentos financieros. Las ICOs han venido ganando importancia frente a las fuentes tradicionales de financiación, como las Ofertas Públicas de Suscripción (OPSs). El problema, sin embargo, radica en que, en ocasiones, las ICOs se utilizan precisamente para el arbitraje regulatorio, a fin de evitar la la normativa del sistema financiero que devendría aplicable en el caso de una OPV. Es más: prácticas prohibidas en el sistema financiero tradicional (como el *spoofing* o el *inside trading*) pueden ser más fáciles de ejecutar en el entorno blockchain. Si no se hace nada respecto a los criptoactivos, podrían convertirse en una fuente impredecible de inestabilidad para la eco-

(38) Véase https://www.statista.com/statistics/730876/cryptocurrency-maket-value/
(39) Véase https://coinmarketcap.com/

nomía mundial. Es necesaria una mínima intervención regulatoria que evite su uso, en la medida de lo posible, como canal de blanqueo de fondos procedentes de actividades ilícitas. Sin embargo, dicha normativa debe garantizar las ventajas de las criptodivisas como activos financieros y medios de pago, reduciendo los costes asociados con la intermediación en el sistema financiero. En los últimos años, y como se explica con mayor profusión en el Capítulo posterior dedicado a esta cuestión, los poderes públicos han reaccionado ante estas disrupciones surgidas del entorno blockchain. En la Unión Europea, el Reglamento 2022/858, sobre régimen piloto para infraestructuras de mercado basadas en tecnología de libro mayor distribuido, y el Reglamento sobre Mercados de Criptoactivos (MiCAR) tratarán de regular los activos representados a través de la tecnología blockchain para minimizar los posibles perjuicios a los inversores y a los sistemas monetarios y financieros en su conjunto. Además, el Banco Central Europeo sigue trabajando en su proyecto de un euro digital, como forma de conceder a los ciudadanos algunas de las ventajas de las criptodivisas, pero manteniendo su soberanía monetaria.[40]

3.3. Intangibilidad de las divisas virtuales por parte de las autoridades

Las criptodivisas no pueden confiscarse o, al menos, es más difícil hacerlo. Los «*smart contracts*» son fragmentos de código autoejecutables y autoaplicables. Una vez que un *smart contract* se codifica en una blockchain, sus disposiciones se cumplirán automáticamente. Si A «firma» un contrato recogido en un *smart contract* por el que promete transferir un Bitcoin a B de forma periódica, una vez llegado el día acordado, el Bitcoin será transferido, independientemente de si A quiere cumplir su promesa o no, y sin recurrir a un tercero (un juez) que haga cumplir el «contrato».

Los *smart contracts* permiten a los particulares entablar relaciones comerciales que no necesitan recurrir a los cauces legales y jurisdiccionales habituales para ser ejecutadas. Esto, sin embargo, implica que estas transacciones son ajenas a los poderes de los Estados. En otras palabras, los actores maliciosos pueden beneficiarse de los contratos inteligentes y de la tecnología blockchain, ya que pueden evitar la confiscación por parte de las autoridades públicas, que no pueden congelar o bloquear esos activos al no poder dar órdenes a un intermediario acreditado para que lo haga, puesto que no existe. Esto otorga una gran ventaja a los poseedores de estos activos cuyo origen es delictivo. En otras palabras, las blockchans permiten que los actores mali-

(40) BCE. Euro Digital. N.d. https://www.ecb.europa.eu/paym/digital_euro/html/index.es.html

ciosos realicen transacciones sofisticadas y representen valor económico en paralelo a las autoridades y la justicia.

3.4. Las criptodivisas como amenaza para la estabilidad política: una herramienta opaca para la financiación de actividades de influencia por parte de los Estados

Un buen ejemplo de cómo las criptodivisas amenazan la estabilidad política nos lo ofrecen las revelaciones incluidas en las investigaciones sobre el hackeo y difusión de los correos electrónicos de la campaña del Partido Demócrata en las elecciones estadounidenses de 2016[41]. Este caso resulta bastante ilustrativo en la medida en que evidencia que los Estados, en sus acciones encubiertas en el ciberespacio, están utilizando Bitcoin como medio de pago totalmente opaco para sufragar los costes de dichas operaciones, evitando complejas estructuras financieras y legales internacionales que impedirían el seguimiento de dichas actividades.

Las agencias estatales están utilizando el mismo sistema que las organizaciones criminales para transferir dinero por la red sin ser detectadas ni dejar rastro. Especialmente significativa en este sentido es la demanda interpuesta el 13 de julio de 2018 por el Departamento de Justicia de Estados Unidos contra 12 agentes de inteligencia rusos, acusados de acceder a correos electrónicos del Comité del Partido Demócrata, la campaña presidencial de la entonces candidata Hillary Clinton y el Comité de Campaña Demócrata del Congreso, siendo acusados de 11 delitos, entre ellos la conspiración de agentes de inteligencia rusos contra Estados Unidos, blanqueo de capitales e intento de asalto a consejos electorales estatales y otros organismos gubernamentales: una clara injerencia en las elecciones presidenciales de 2016. De la denuncia se deduce que el uso de Bitcoin constituyó una parte esencial en el desarrollo de la operación, ya que permitió realizar todos los pagos imposibilitando su seguimiento. De acuerdo con el texto de la denuncia:

> *«In early 2016, Russian intelligence officers obtained a new pool of the virtual currency Bitcoin. They quickly put the digital money to work. The Russian spies used some of the Bitcoins to pay for the registration of a website, dcleaks.com, where they would later post emails that had been stolen from Hillary Clinton's presidential cam-*

(41) WASHIGNTON POST. La investigación de Mueller acusa a 12 rusos de hackear a demócratas en 2016. 2018. https://www.washingtonpost.com/world/national-security/rod-rosenstein-expected-to-announce-new-indictment-by-mueller/2018/07/13/bc565582-86a9-11e8-8553— a3ce89036c78_story.html?utm_term=.8af9be7cf433

paign. When the operatives needed a computer server to host the dcleaks site, they paid for that with Bitcoins as well[42]».

El punto más interesante es la acusación relacionada con el uso de Bitcoin como medio de pago y, sorprendentemente, al mismo tiempo como medio de financiación de operaciones a través de la minería de Bitcoins por parte de la GRU (inteligencia militar rusa):

«*8. To hide their connections to Russia and the Russian government, the conspirators used false identities and made false statements about their identities. To further avoid detection, the conspirators used a network of computers located across the world, including in the United States, and paid for this infrastructure using cryptocurrency.*

58. Although the conspirators caused transactions to be conducted in a variety of currencies, including U.S. dollars, they principally used Bitcoin when purchasing servers, registering domains and otherwise making payments in furtherance of hacking activity. Many of these payments were 21 processed by companies located in the United States that provided payment processing services to hosting companies, domain registrars and other vendors both international and domestic. The use of Bitcoin allowed the conspirators to avoid direct relationships with traditional financial institutions, allowing them to evade greater scrutiny of their identities and sources of funds».

De esta manera nos encontramos ante el primer caso conocido de una investigación sobre el uso de Bitcoin en actividades encubiertas por parte de una agencia de inteligencia estatal. En este caso fue el GRU, con el objetivo de influir en el proceso democrático de las elecciones presidenciales estadounidenses. Se trata de una injerencia evidente en los asuntos internos del proceso político estadounidense que constituye una amenaza para la libertad y la independencia de un Estado soberano procedente de otro, así como una grave amenaza para la seguridad nacional[43].

(42) NEW YORK TIMES. 12 agentes rusos acusados en la investigación de Mueller. 2018. https://www.nytimes.com/2018/07/13/us/politics/mueller-indictment-russian-intelligence-hacking.html?rref=collection%2Fsectioncollection%2Fpolitics&action=click&contentCollection=politics&region=rank&module=package&version=highlights&contentPlacement=2&pgtype=sectionfront

(43) Ibid.
The Bitcoin network allows anyone to move millions of dollars across the world without any in-person meetings, and without the approval of any financial institutions. First released in 2009 by its mysterious creator, Satoshi Nakamoto, Bitcoin was designed to operate without any central authority that could block transactions or verify the identities of the people involved. All Bitcoin transactions and wallets are recorded on a database known as the Blockchain, by a network of computers that anyone can join. The unusual structure has long made Bitcoin a primary means of payment for drugs on online black markets, and more recently as a method for making ransom payments.

En la denuncia se afirma que la inteligencia rusa «*principally used Bitcoin when purchasing servers, registering domains and otherwise making payments in furtherance of hacking activity* (...) (Bitcoin)*allowed the conspirators to avoid direct relations with traditional financial institutions, allowing them to evade greater scrutiny of their identities and sources of funds*».

También es especialmente interesante la forma en que operaban en el mercado de Bitcoin para ocultar los movimientos:

> «*The Russians took several steps to obscure their Bitcoin transactions, according to the indictment. They bought some Bitcoins on so-called peer-to-peer exchanges, where buyers and sellers can interact directly without exchanges collecting details on either side*».

Y también es muy relevante la descripción que se hace en la querella de cómo se financiaba la operación con la minería de Bitcoins:

> «*The Russians also created Bitcoins themselves through the process known as mining, the indictment said. With mining, computers compete to unlock new Bitcoins by solving difficult computational problems. This requires expensive equipment and lots of electricity, but that was apparently not a hindrance to the Russians*[44]».

La denuncia señala finalmente que el uso de Bitcoins financió la infraestructura informática necesaria para llevar a cabo la operación. Incluyó el pago del servidor ubicado en Malasia que alojaba la web creada para filtrar correos electrónicos, dcleaks.com, y el pago a una empresa rumana para registrar el citado dominio. En definitiva, una operación de influencia con un gran poder disruptivo en el ámbito político y mediático que, gracias a la realidad, digital pudo llevarse a cabo por unos pocos miles de dólares y con la garantía de un anonimato casi total. Sólo se ha desvelado tras meses de investigación y gracias a los grandes recursos de la NSA y otras agencias de inteligencia occidentales.

En este sentido, se deduce que, sin desvelar la forma, la inteligencia americana ha sido capaz de reconstruir los pasos dados en el uso de Bitcoins probablemente utilizando algún tipo de desarrollo que permita descubrir las operaciones anónimas en los cripto-sistemas basados en blockchain.

(44) Ibid.
In March 2016, the indictment said, the Russians also used Bitcoin to buy a so-called virtual private network account that allowed them to obscure their internet protocol address and their location when they went online. They used that VPN account to operate a Twitter account known as Guccifer_2, which became infamous after releasing some of the emails stolen from the Democratic National Committee and of the chairman of the Clinton campaign, John D. Podesta.

En lo que respecta a España, las criptodivisas se utilizaron como vehículo de pago para el referéndum ilegal catalán del 1 de octubre de 2017. El Govern de Cataluña, la Generalitat, sufragó, a través de Bitcoins, algunos dominios de internet para lanzar su página web. También destinó pagos a Amazon a cambio del desarrollo de la plataforma para el escrutinio de la votación. La Generalitat eligió este método de pago por el carácter ilícito del referéndum y el origen (público) de los fondos empleados, por lo que bancos y demás instituciones financieras no habrían accedido a llevar estas operaciones a cabo. El uso de Bitcoin permitió a la Generalitat cumplir sus objetivos sin recurrir a intermediarios[45], sorteando el cumplimiento de la normativa.

Otra posible amenaza contra la Seguridad Nacional derivada de la tecnología blockchain proviene del uso ilegítimo como medio de identificación de los ciudadanos en sus relaciones con las administraciones públicas. En concreto, este supuesto se ha puesto de manifiesto en la aprobación del Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones en España, que prohíbe el uso de blockchain como mecanismo de verificación de la identidad de los ciudadanos en relación con los gobiernos autonómicos, hasta que la Unión Europea regule esta cuestión. Así, se pretende evitar el uso de blockchain para construir sistemas de identificación que suplanten a los legalmente establecidos a nivel estatal con carácter exclusivo *ex lege*.

3.5. Robo de criptodivisas

Otro riesgo está directamente relacionado con la seguridad de las criptodivisas. A pesar de que una de las principales ventajas de las cadenas de bloques —especialmente, de las grandes *blockchains*— es la protección que ofrecen frente a ataques maliciosos, también presentan algunas debilidades que pueden hacerlas vulnerables. Cuando los usuarios recurren a *hot wallets*, estos proveedores se convierten en los guardianes últimos de las claves criptográficas. Cuanto mayor es el tamaño de un proveedor de *hot wallets*, mayores son los incentivos asociados a un ciberataque. Esto explica por qué durante los últimos años, tantos *hot wallets* han sido víctimas de hackeos multimillonarios. A partir de 2019, Corea del Norte centró especialmente sus campañas de ciberataques con ánimo de lucro en las plataformas de intercambio de criptodivisas. El informe de la ONU de 2019 des-

(45) EL MUNDO. El Govern usó Bitcoins para ocultar gastos del referéndum. 2017. http://www.elmundo.es/cataluna/2017/11/24/5a1742c322601ddd758b45de.html

cribe cómo la plataforma de intercambio «Bithumb» fue atacada cuatro veces por Corea del Norte, lo que resultó en pérdidas totales de aproximadamente 60 millones de dólares[46].

Los ciberataques dirigidos contra *hot wallets*, y a las plataformas de intercambio, están relacionados con las *blockchains*, pero son externos a ellas (ocurren «*off-chain*»). Algunos ataques, sin embargo, aprovechan vulnerabilidades de las propias cadenas de bloques («*on-chain*»). Las iniciativas descentralizadas desarrolladas sobre tecnología *blockchain* suelen hacer uso de código de fuente abierta. Esto tiene la ventaja de permitir que diferentes individuos y grupos aúnen esfuerzos y contribuyan a la mejora del *software*; sin embargo, también puede revelar posibles vulnerabilidades frente a los actores maliciosos. TheDAO era un proyecto basado en Ethereum que intentaba replicar el funcionamiento de un fondo de inversión, pero organizado de forma descentralizada, operando simplemente a través de *smart contracts*. Los particulares podían «invertir» sus fondos en TheDAO, recibiendo, a cambio, un token que tenía asociados derechos similares a los de las acciones. Los fondos recaudados por TheDAO se invertían en diferentes proyectos. Los propietarios de los tokens TheDAO podían decidir qué proyectos financiar (derechos políticos), y recibían beneficios de los ingresos procedentes de las inversiones (derechos económicos). En 2016, un atacante desconocido aprovechó una vulnerabilidad no detectada en TheDAO y transfirió casi 60 millones de dólares en fondos a su cuenta personal. Como la operación se realizó de acuerdo con el código informático de los *smart contracts*, la operación era —teóricamente— imposible de revertir. Para poder recuperar los fondos de los *tokenholders* de TheDAO, la mayoría de la comunidad Ethereum acordó restaurar blockchain de Ethereum al momento anterior al hackeo. Este movimiento fue tremendamente controvertido, ya que se oponía al principio básico de inmutabilidad de las cadenas de bloques, y provocó la bifurcación («*hard fork*») entre Ethereum y Ethereum Classic[47].

Una forma relativamente reciente de ataque destinado a producir beneficios económicos que se basa intrínsecamente en la tecnología blockchain es el conocido como «*cryptojacking*». Mediante el cryptojacking, los dispositivos infectados comienzan a minar criptodivisa (normalmente, Monero o Bitcoin) por cuenta de los atacantes, «parasitando» los equipos afectados.

(46) CONSEJO DE SEGURIDAD DE LA ONU. Op. cit. p. 28.

(47) GEMINI. ¿Qué fue el DAO? Marzo 2022. https://www.gemini.com/cryptopedia/the-dao-hack— makerdao#section-the-dao-hack-remedy-forks-ethereum

Estos ejemplos evidencian cómo el robo de criptoactivos tanto *off-chain* como *on-chain* constituye una actividad muy lucrativa.

4. BLOCKCHAIN Y CONSUMO DE ENERGÍA

Un aspecto colateral vinculado a blockchain es el elevado consumo de energía que ha caracterizado tradicionalmente a esta tecnología. Esto se debe al mecanismo utilizado por varias blockchains (como Bitcoin) para lograr el consenso y garantizar la protección frente a actores maliciosos: la prueba de trabajo («*Proof-of-Work*», o PoW). Explicado de forma simple, para añadir nuevos bloques a blockchain de Bitcoin, un nodo «minero» tiene que demostrar que ha «consumido» cierta cantidad de electricidad. A cambio del coste de esa electricidad, el minero recibe nuevos Bitcoins. Entre otras ventajas, el PoW disuade a potenciales actores de amenazas dispuestos a apoderarse de toda blockchain y crear nuevos Bitcoins para sí mismos, ya que esta creación estará asociada a altos costes derivados de la electricidad «desperdiciada». El lado negativo, por supuesto, reside en el consumo de energía de las cadenas de bloques basadas en PoW. Así, se afirma que en 2014 el consumo estimado de Bitcoin era comparable al de toda Irlanda. En la actualidad, el consumo anual de energía de Bitcoin supera al de países enteros como Bélgica o Pakistán. De hecho, sólo 33 países en todo el mundo consumen más energía que la cadena de bloques Bitcoin. Además, se trata de un proceso incremental, ya que, cuanto mayor es la cotización de la divisa digital, más consumo de energía se necesita a medida que aumentan las transacciones y el número de mineros. A su vez, los ingresos se reinvierten en generar más criptodivisas. Esto tiene un claro impacto en la seguridad energética de los países, que forma parte de las estrategias de seguridad nacional como un componente de vital importancia. También tiene graves consecuencias medioambientales, ya que, aunque el consumo de energía de las redes de divisas virtuales crece exponencialmente año tras año, la producción mundial de energía no puede crecer de la misma manera. Un posible aumento del precio de la energía podría restringir el acceso a otros agentes económicos de la economía no financiera, o a sectores sociales con menor poder adquisitivo que quedarían excluidos del consumo energético.

Sin embargo, las cadenas de bloques más recientes han evolucionado a partir del protocolo de consenso PoW, desarrollando modelos alternativos que pueden garantizar un nivel equivalente de seguridad al tiempo que disminuyen sustancialmente el consumo de energía. En septiembre de 2022, blockchain Ethereum acordó cambiar su protocolo de PoW al denominado

«*Proof-of-Stake*» (PoS). En PoW, los mineros deben demostrar que han gastado cierta cantidad de energía para añadir nuevos bloques. Con PoS, los mineros deben demostrar que han adquirido cierta cantidad de criptodivisa (Ether, en el caso de Ethereum) para añadir nuevos bloques. Sin embargo, no se desperdicia ningún bien externo a blockchain (como la electricidad). Se estima que el cambio a un protocolo PoS puede reducir el consumo de energía de Ethereum en un 99,5%[48].

Al tratarse de una innovación reciente, se requerirá de tiempo para estudiar la evolución de los protocolos PoS, y si es adoptada por más blockchains o no. Solo entonces podremos saber si el problema del consumo energético de las blockchains ha sido resuelto por el propio mercado, o si sigue siendo necesaria una intervención pública externa.

5. BLOCKCHAIN COMO GARANTÍA DE LAS CADENAS DE SUMINISTRO

Otra aplicación de la tecnología blockchain con conexión directa con la seguridad nacional está vinculada a las cadenas de suministro desplegadas a nivel global. Las complejas relaciones comerciales y productivas de la economía global hacen que los productos (especialmente los tecnológicos) operen mediante cadenas de producción en las que intervienen diferentes socios de distintos países. Una de las tecnologías que puede ayudar a asegurar el origen y los componentes de estos suministros en sus diferentes fases es el blockchain, que puede añadir veracidad y certidumbre en la cadena de suministro, evitando así el fraude o la introducción de elementos maliciosos en procesos productivos complejos. Estas garantías pueden contribuir a la fiabilidad y seguridad, contribuyendo, en último término, a elevar la seguridad de los Estados (especialmente, en relación con los suministros más sensibles como son los relacionados con sistemas y redes identificados como esenciales para la defensa nacional o como infraestructuras críticas). Una de las principales ventajas de los sistemas basados en blockchain radica en su capacidad para verificar la autenticidad e integridad de los componentes que se integran en complejas cadenas de suministro. La combinación de sellos criptográficos junto con funciones no clonables hace que la confianza entre las partes implicadas en estos procesos productivos sea mucho mayor ya que, en muchos casos, es necesario cumplir con protocolos y estándares de seguridad rigurosos e inflexibles. Estos se garantizan desde el inicio de la producción, y en todas las fases sucesivas. Según datos publicados, el aumento

(48) Véase https://ethereum.org/en/energy-consumption/

de la ciberseguridad en las cadenas de suministro preocupa al 86% de las empresas del sector aeronáutico y espacial, que buscan activamente respuestas a través de la tecnología blockchain[49]. Garantizar la trazabilidad de todos los elementos que se incorporan a esa cadena de suministro es una gran baza a la hora de asegurar la ausencia de intrusiones ocultas.

Particularmente, en el campo de la ciberdefensa y el resto de sistemas al servicio de la ciberseguridad, la cadena de bloques puede ser enormemente útil, sobre todo porque puede garantizar la resiliencia de las comunicaciones. El diseño de esta tecnología permite comunicaciones seguras y resistentes en situaciones en las que la seguridad de los datos y de la red podría verse comprometida. El espectro radioeléctrico puede convertirse en un teatro de operaciones en el que se producirían acciones encaminadas a interrumpir las comunicaciones y robar o manipular datos (especialmente en lo que respecta a sistemas de comunicación críticos como satélites, cables submarinos o enlaces de datos tácticos). Por lo tanto, la capacidad de generar, proteger y compartir datos de forma segura será fundamental en el campo de batalla actual. Las blockchains pueden mejorar notablemente esa capacidad gracias a sus propios protocolos de seguridad, que incluyen su sistema de mensajería, la adaptabilidad al uso de diversos medios de comunicación, la base de datos distribuida y el mecanismo de consenso. Al no existir un nodo maestro en la red, la interrupción es mucho menos probable. La red seguiría operando aunque una parte importante de la misma se viera afectada por un ataque.

6. BLOCKCHAIN Y EL INTERNET DE LAS COSAS (IOT)

También en este ámbito, la tecnología blockchain puede contribuir de forma enormemente significativa a aumentar el nivel de ciberseguridad. Como se afirma de modo rotundo; «existe un consenso creciente entre las compañías tecnológicas relativo al carácter esencial de blockchain para alcanzar el potencial del Internet de las Cosas»[50].

La expansión global del uso de dispositivos conectados constituye una gran amenaza para la ciberseguridad; se calcula que hay aproximadamente 14.400 millones de dispositivos conectados por *IoT* en todo el mundo. No obstante, la ciberseguridad de estos dispositivos no ha destacado, tradicio-

(49) FORBES. Accenture muestra un prototipo de Blockchain para cadenas de suministro aeroespaciales en el Salón Aeronáutico de Farnborough. 2017. https://www.forbes.com/consent/?toURL=https://www.forbes.com/sites/astanley/2018/07/16/accent ure-showcases-Blockchain-prototype-for-aerospace-supply-chains-at-farnborough-air-show/

(50) TAPSCOTT, D., *Revolución Blockchain*, 2016. p. 153.

nalmente, como una prioridad para sus fabricantes, por lo que suelen tener una seguridad moderada o baja[51]. Además de la falta de robustez del diseño, esta realidad se debe, entre otras razones, al uso de contraseñas predeterminadas o débiles, la ausencia de cifrado o las escasas actualizaciones de *software* para parchear vulnerabilidades.

Estas vulnerabilidades se explotaron especialmente durante 2017, permitiendo utilizar los dispositivos *IoT* como herramientas para llevar a cabo ciberataques (*IoT* en *botnets*), así como para espiar a sus usuarios o manipular su entorno. En noviembre, por ejemplo, 900.000 clientes de Deutsche Telekom fueron víctimas de la *Botnet Mirai*, que infectó routers *Speedport*, provocando el fallo de su conexión a Internet.

La seguridad de los dispositivos IoT supone una cuestión crucial en estos momentos para aumentar la ciberseguridad de nuestras sociedades y que afecta directamente a la vida de los ciudadanos, ya que son los propietarios de estos dispositivos que se utilizan como vectores de ataque. Por ello, la Comisión Europea, consciente del problema, publicó en septiembre de 2022 una Propuesta de Reglamento sobre requisitos horizontales de ciberseguridad para productos con elementos digitales, también conocida como «*Cyber Resilience Act*» (CRA)[52]. Esta Propuesta prevé obligaciones de ciberseguridad para fabricantes, importadores y distribuidores de dispositivos con elementos digitales y su *software*.

El uso de blockchain permite aumentar el control de estos dispositivos tanto en lo que se refiere a la cadena de montaje como a su control una vez conectados:

> «*To enable and improve situational awareness of IoT devices and critical infrastructure, adoption of innovative blockchain capabilities that augment traditional solutions is necessary. This innovative approach augments traditional security monitoring and mitigation capabilities and provides distributed, continuous monitoring of IoT devices, endpoints, and assets enriched with immutable, tamperproof, and cryptographically signed transaction data. IoT device sensors and critical infrastructure endpoints and assets feed blockchain capabilities, enabling devices to participate in secure monitoring of transactions. Devices will be able to communicate with*

(51) CNN. Ciberamenazas y tendencias edición 2018. 2018. https://www.ccn— cert.cni.es/informes/informes-ccn-cert-publicos/2835-ccn-cert-ia-09-18-ciberamenzas-y-tendencias — edicion-2018-1/file.html

(52) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52022PC045

enterprise-defined, blockchain-based ledgers that autonomously collect, manage, and analyze, through SmartContracts, the security hygiene of endpoints[53]».

Es decir, se puede producir un cambio de paradigma en la ciberseguridad de estos dispositivos, ya que un enfoque basado en blockchain permitiría contrastar con el actual sistema tradicional de centralización de las capacidades de seguridad, a la vez que aumentaría la capacidad de hacer inteligencia de ciberseguridad de forma compartida a lo largo de toda la cadena.

Quizás, lo más relevante sea la aplicación de esta tecnología al desarrollo de las *Smart cities*, que sólo será posible mediante el despliegue de un enorme número de dispositivos conectados que puedan generar y explotar datos para hacer más eficiente la gestión de las ciudades. Esta es, a su vez, la mayor vulnerabilidad del esquema ya que, como se ha mencionado anteriormente, estos dispositivos *IoT* no han sido objeto de inversiones en ciberseguridad demasiado significativas, ya que, hasta ahora, los incentivos han sido escasos. En definitiva, el reto de proteger estas ciudades inteligentes es serio. Una vez más, en este ámbito, la credencial de seguridad basada en blockchain puede ser de gran ayuda, permitiendo que sólo los dispositivos *IoT* con dicha certificación puedan conectarse a la red, conexión que sólo puede ser posible una vez que dicha certificación haya sido validada a través de los mecanismos de consenso de la cadena. La cuestión es especialmente relevante en relación con el despliegue de las redes 5G, que implica la extensión de miles de *Smart cells* para hacer posibles cambios tan importantes en nuestras vidas como la conducción autónoma.

El proceso ha suscitado todo tipo de cuestiones polémicas en las que el aspecto de la seguridad nacional ha sido fundamental a la hora de plantear los problemas de ciberseguridad del despliegue de las nuevas redes[54]. En este sentido, cabe destacar cómo la ciberseguridad de estas nuevas redes 5G pasa a un primer plano como una cuestión crucial de seguridad nacional debido a la preocupación de las autoridades estadounidenses por la posibilidad de que dichas redes se construyan sobre la base de tecnología y dispositivos chinos, ya que dos de los mayores fabricantes mundiales de estas *Smart cells* proceden de China, y siendo una de ellas de titularidad estatal. Esto ha suscitado un acalorado debate sobre la posibilidad, propuesta incluso por algunos asesores de seguridad nacional, de que el despliegue de estas

(53) Véase https://www.ibm.com/blogs/insights-on-business/government/convergence-Blockchain— cybersecurity/

(54) CNBC. El Tesoro cita la seguridad nacional y la competencia por el 5G como riesgos en la alianza Qualcomm-Broadcom. 2018. https://www.cnbc.com/2018/03/06/treasury-cites-national-security-and— competition-for-5g-as-risks-in-qualcomm-broadcom-tieup.html

redes no corra a cargo de empresas privadas, sino del Gobierno federal. Se teme que un despliegue con equipos ya infectados en infraestructuras de comunicaciones privadas pueda tener en el futuro efectos letales que pongan en peligro las infraestructuras físicas o la vida de los ciudadanos.

Lo cierto es que, aunque existan dudas sobre la fiabilidad de este tipo de equipos por su origen, las blockchains pueden ayudar a aumentar la seguridad. A través de sus certificaciones, que se aplican a toda la cadena de suministro de estos dispositivos, las blockchains pueden ser muy útiles para demostrar la confianza en estos dispositivos, facilitando el despliegue seguro de las redes 5G. Se estima que el mercado del 5G alcanzará el valor de 1,67 billones de dólares en 2030[55].

7. CONCLUSIONES

1.- Quince años después de la creación de la primera cadena de bloques, esta tecnología sigue en desarrollo. Las *blockchains* más recientes tratan de solventar algunas de las limitaciones de las versiones anteriores (como el consumo de energía). Además, periódicamente surgen nuevos casos de uso para la tecnología blockchain.

2.- A lo largo de este tiempo, esta tecnología de libro mayor distribuido ha demostrado que puede utilizarse para mantener registros de datos con un alto grado de integridad.

3.- La importancia potencial de esta tecnología es enorme porque, en nuestras sociedades, la información y los datos se han vuelto omnipresentes y cruciales para configurar nuestra forma de vida. Esa relevancia aumentará a medida que los avances en IA permitan que los ciberataques sean cada vez más sofisticados.

4.- Las consecuencias de su uso para la seguridad nacional son múltiples y diversas, y van desde el impacto energético hasta la estabilidad financiera.

5.- El impacto potencial de las criptodivisas, y de los criptoactivos en general, sigue siendo desconocido. Mientras que la alta volatilidad de los precios impide que las criptodivisas actuales se conviertan en un sustituto del dinero *fiat*, nuevos desarrollos como las stablecoins pueden solventar, al menos parcialmente, estas limitaciones en el futuro. Las ICOs, por su parte, son ya un sólido canal de financiación.

(55) Véase https://www.ericsson.com/en/press-releases/2020/11/ericsson-estimates-usd-31-trillion-5g— consumer-market-by-2030

6.- La tecnología blockchain permite a agentes maliciosos, incluidos Estados y grupos delictivos, transmitir, recibir y blanquear representaciones de valor económico.

7.- Las autoridades públicas intentan responder a las amenazas que plantea la tecnología blockchain.

8.- La Unión Europea ha sido pionera en la regulación de los intermediarios que participan en el ecosistema blockchain, estableciendo obligaciones relativas a la prevención del blanqueo de capitales. El Reglamento MiCA es el mayor exponente de esta tendencia.

9.- Las autoridades policiales están combatiendo activamente la «infraestructura gris» que facilita el trabajo de los actores maliciosos, como demuestra el desmantelamiento por parte del FBI de mezcladores y plataformas de intercambio utilizados para facilitar el blanqueo de capitales.

10.- La colaboración internacional es esencial para el éxito en esta lucha.

11.- Gracias a Blockchain surgirán nuevas oportunidades para aumentar nuestra seguridad y nuestro desarrollo económico y social. Estos hitos digitales, no obstante, irán inevitablemente emparejados a nuevos riesgos y amenazas.

BIBLIOGRAFÍA

AIBC. Genesis Block Day: Bitcoin turns 14. Jan. 2023. https://aibc.world/news/genesis-block-day-Bitcoin-turns-14/#:~:text=%E2%80%9CThe%20Times%2003%2FJan%2F,of%20a%20bank%20bailout%20broke

BBC. US fuel pipeline hackers «didn't mean to create problems. May 2021. https://www.bbc.com/news/business-57050690

CNN. Ciberamenazas y tendencias edición 2018. 2018. https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2835-ccn-cert-ia-09-18-ciberamenzas-y-tendencias-edicion-2018-1/file.html

CHAINANALYSIS. DeFi Takes on Bigger Role in Money Laundering But Small Group of Centralized Services Still Dominate. Jan 2022. https://blog.chainalysis.com/reports/2022-crypto-crime-report-preview-cryptocurrency-money-laundering/

CNBC. Treasury cites national security and competition for 5G as risks in Qualcomm-Broadcom tie-up. 2018. https://www.cnbc.com/2018/03/06/treasury-cites-national-security-and-competition-for-5g-as-risks-in-qualcomm-broadcom-tieup.html

DEPARTAMENTO DE SEGURIDAD NACIONAL, Informe Anual de Seguridad Nacional 2021. P43. https://www.dsn.gob.es/es/documento/informe-anual-seguridad-nacional-2021

DOJ. Justice Department Investigation Leads to Takedown of Darknet Cryptocurrency Mixer that Processed Over $3 Billion of Unlawful Transactions. March 2023. https://www.justice.gov/opa/pr/justice-department-investigation-leads-takedown-darknet-cryptocurrency-mixer-processed-over-3

DOJ. FBI disrupts virtual currency exchanges used to facilitate criminal activity. Apr. 2023. https://www.justice.gov/usao-edmi/pr/fbi-disrupts-virtual-currency-exchanges-used-facilitate-criminal-activity

ECB. Euro Digital. N.d. https://www.ecb.europa.eu/paym/digital_euro/html/index.es.html

EL MUNDO, http://www.elmundo.es/cataluna/2017/11/24/5a1742c322601ddd758b45de.html

ENISA. Distributed ledger tecnology & cybersecurity. Dec. 2016.

ENISA. ENISA Threat Landscape 2022. 2022. P. 15. https://www.einsa.europa.eu/publications/enisa-threat-landscape-2022.

ERICSSON. Ericsson estimates USD 31 trillion 5G consumer market by 2030. Nov. 2017. https://www.ericsson.com/en/press-releases/2020/11/ericsson-estimates-usd-31-trillion-5g-consumer-market-by-2030

EUROPEAN PARLIAMENT. Virtual currencies. Monetary Dialogue July 2018. European Parlament. PE 619.016.

EUROPEAN PARLIAMENT. How blockchain technology could change our lives. In Depth Analysis. European Parliamentary Research Service. Feb. 2017.

EUROPOL. IOCTA 2021. P. 37. https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf

FELIU ORTEGA, L. «La ciberseguridad y la ciberdefensa», *Monografías del CESEDEN*, NÚM. 126, Ministerio de Defensa, 2011. P. 41.

FINTECHRU. Russia's FSB is making life harder for Blockchain companies. Jul. 2020. https://www.fintechru.org/publications/russia-s-fsb-is-making-life-harder-for-blockchain-companies/

FORBES. Accenture showcases blockchain prototype for aerospace supply chains at Farnborough Air Show. 2017. https://www.forbes.com/consent/?toURL=https://www.forbes.com/sites/astanley/2018/07/16/accenture-showcases-blockchain-prototype-for-aerospace-supply-chains-at-farnborough-air-show/

GARCÍA MEXÍA, P., *El Derecho de Internet*, Atelier libros jurídicos, 2016. Page 23.

GEMINI. What Was The DAO? March 2022. https://www.gemini.com/cryptopedia/the-dao-hack-makerdao#section-the-dao-hack-remedy-forks-ethereum

GÓMEZ DE ÁGREDA, A., «El ciberespacio como escenario de conflicto. Identifying Threats», *CESEDEN Monographs*, No. 126, Ministry of Defence, 2011. Page 180.

KALDOR, M., *Las nuevas guerras*, Tusquets, Madrid, 2001. Page 15.

KASPERSKY, https://www.kaspersky.com/resource-center/threats/blackenergy

KELSEN, H., *General State Theory*. Editorial Nacional, Mexico, 1979. Page 55.

LIBICKI, M., *Cyberdeterrence and cyberwar*. Rand Corporation, Santa Mónica, 2009. Pág. 12.

McKenzie, Timothy M. Is Cyber Deterrence Possible? 2017. P. 14. https://media.defense.gov/2017/Nov/20/2001846608/-1/-

NORTON. Cyber Safety Insight Report. 2022 https://www.nortonlifelock.com/us/en/newsroom/press-kits/2022-norton-cyber-safety-insights-report-special-release-online-creeping/

TAPSCOTT, D. *Blockchain revolution*. 2016.

THE ECONOMIST. Defending the digital frontier. 12 Jul 2014.

THE ECONOMIST. Digital detergent, April 28th 2018.

THE NEW YORK TIMES, retrieved from https://www.nytimes.com/2018/04/29/technology/blockchain-iso-russian-spies.html

NEW YORK TIMES.12 Russian Agents Indicted in Mueller Investigation. 2018. https://www.nytimes.com/2018/07/13/us/politics/mueller-indictment-russian-intelligence-hacking.html?rref=collection%2Fsectioncollection%2Fpolitics&action=click&contentCollection=politics&region=rank&module=package&version=highlights&contentPlacement=2&pgtype=sectionfront

WALL STREET JOURNAL. Cryptocurrency Can Promote National Security. Dec. 2017. https://www.wsj.com/articles/cryptocurrency-can-promote-national-security-1513280417

UN SECURITY COUNCIL Report S/2019/691. 2019. P. 26. https://www.securitycouncilreport.org/atf/cf/%7b65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7d/S_2019_691.pdf

VICE. Experts Doubt Russian Claims That Cryptographic Flaw Was a Coincidence. May. 2019. https://www.vice.com/en/article/43j3wm/experts-doubt-russian-encryption-estándar-cryptography-backdoor-streebog-kuznyechik

WASHIGNTON POST. Mueller probe indicts 12 Russians with hacking of Democrats in 2016. 2018. https://www.washingtonpost.com/world/national-security/rod-rosenstein-expected-to-announce-new-indictment-by-mueller/2018/07/13/bc565582-86a9-11e8-8553-a3ce89036c78_story.html?utm_term=.8af9be7cf433

WIRED. The Untold Story of NotPetya, the Most Devastating Cyberattack in History. Aug. 2022. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/