Ciberseguridad económica

Antonio Fonfría | Universidad Complutense de Madrid.

Néstor Duch-Brown | Centro Común de Investigación (JRC, por sus siglas en inglés) de la Comisión Europea.

Tema

La ciberseguridad posee unos condicionantes económicos vinculados a la seguridad económica que han sido muy poco explorados. Tanto los costes asociados a los riesgos de ciberseguridad como las inversiones necesarias para prevenirles precisan una mayor atención y metodología de análisis.

Resumen

La seguridad económica es un concepto aún difuso. Su importancia es difícil de soslayar debido a que la economía impregna todas las actividades sociales. Los costes y beneficios derivados de diversas tomas de decisiones han de considerar los factores de seguridad y resiliencia de las economías. El problema resulta más complejo cuando buena parte de las actividades económicas se realizan en espacios virtuales cuyo control es, en el mejor de los casos, difuso. La ciberdelincuencia y los ciberataques representan actividades de elevado beneficio y reducido coste para quienes las realizan y, sin embargo, los costes económicos que sufren las empresas, personas físicas e instituciones públicas pueden ser elevados y, los costes sociales, de una gran entidad.

Análisis

La ciberseguridad es esencial tanto las para empresas, como para los gobiernos y los individuos. La creciente digitalización de la actividad económica impulsa negocios, abre mercados nuevos o mejora la productividad empresarial, pero al mismo tiempo genera riesgos como el espionaje o la explotación de las vulnerabilidades en el software, entre otros, que facilitan nuevas vías para la ciberdelincuencia, los ataques a infraestructuras críticas o fraudes de todo tipo.

Desde la perspectiva económica, los distintos mercados que se encuentran vinculados a través de Internet –productores de software, proveedores de servicios, redes sociales, usuarios, es decir, la demanda, entre otros–, muestran características muy diversas que requieren un tratamiento específico que no se observa en la mayor parte de los sectores económicos y su funcionamiento, tal y como se concebían tradicionalmente. Esta situación implica la existencia de imperfecciones de mercado de diversa índole, que se conjugan en la *red* y que precisan un enfoque de seguridad económica.

El concepto de seguridad económica en el ciberespacio

La seguridad económica es una parte de la economía a la cual no se le ha prestado suficiente tradicionalmente la suficiente atención, aunque en los últimos 15 años ha comenzado a ser objeto –marginal– de estudio por parte de algunos autores e instituciones. Sin embargo, aún se encuentra fuera del *mainstream* de la economía y el concepto carece de una definición. En este sentido, la OCDE la define como un grupo caleidoscópico de actividades relacionadas con la prevención o la reducción de riesgos tanto de la vida, como de la propiedad[1]. La amplitud de esta definición y su enorme campo de aplicación le resta profundidad y utilidad. Por su parte, la seguridad económica puede definirse como "aquellas actividades afectadas por, y orientadas a la prevención, el tratamiento y la mitigación de la inseguridad en la economía" según Brück[2]. Desde este punto de vista, es un bien público y, como tal, posee las características de no exclusión y no rivalidad en el consumo, generando externalidades positivas. Esto implica la intervención del sector público a fin de obtener el nivel adecuado de seguridad con un uso eficiente de los recursos, tanto públicos, como privados.

Brück, Karaisl y Schneider[3] exponen que la seguridad económica se refiere a la aplicación de herramientas económicas al análisis del origen y la dinámica de la inseguridad. Sin embargo, su aplicación a la ciberseguridad sería muy restrictiva debido a que, tal y como muestran las complejidades que se vienen observando en los distintos mercados *online*, no se dispone de suficientes instrumentos para el conocimiento y control de las numerosas actividades y empresas implicadas. Desde otra perspectiva, Anderson, Böhme, Clayton, y Moore[4] exponen que numerosos fallos de seguridad poseen causas económicas, lo cual puede deberse a que las organizaciones no son plenamente conscientes de los costes que pueden provocar los riesgos de seguridad asumidos. Esto es particularmente importante en el caso del ciberespacio, ya que la inversión en ciberseguridad tendería a reducir dichos riesgos y los efectos económicos negativos que pudieran generar. La inseguridad económica tiende a transmitirse entre sectores, instituciones e individuos, poniendo en mayor riesgo a los eslabones más débiles de la cadena y amplificando sus efectos al conjunto de los agentes implicados.

Desde una posición más pragmática y concreta, Fonfría[5], considera que la seguridad económica forma parte de las actividades de inteligencia económica dirigidas a la seguridad de diversos agentes y a los efectos que su inseguridad puede generar sobre otros o sobre el conjunto de la sociedad. Adicionalmente, se nutre de los resultados de

[1] La Organización para la Cooperación y el Desarrollo Económicos (OCDE), The Security Economy, Capítulo 1, 2004.

[2] Tilman Brück, "An Economic Analysis of Security Policies", *Defence and Peace Economics*, vol. 16 (5), 2005, p. 376.

[3] Tilman Brück, Marie Karaisl y Friederich Schneider (2008), "A Survey of the Economics of Security", *Economics of Security Working Paper* nº 1, 2008.

[4] Ross Anderson y otros, "Security Economics and the Internal Market", European Network and Information Security Agency (ENISA), 2008.

[5] Antonio Fonfría (2020), "Seguridad económica y COVID-19: la necesidad de una estrategia", *Documento de Opinión* 54/2020, Instituto Español de Estudios Estratégicos (IEEE), p. 6.

análisis económicos de diversa índole para apoyar la toma de decisiones tanto económicas, como políticas y empresariales.

Una de las cuestiones claves para determinar la probabilidad y el coste de la ciberseguridad es el conocimiento de los costes que genera y su distribución. Obviamente la seguridad total no existe, por lo que la comprensión de los distintos tipos de costes apoya la toma de decisiones sobre cuales han de ser tratados de manera prioritaria frente a otros, en función de las dos variables mencionadas. En definitiva, sería necesario un análisis de inteligencia económica de la ciberseguridad (cibereconomía) cuyo objetivo sea minimizar tanto su probabilidad como su impacto económico y social. De ello se derivan las políticas y estrategias necesarias para impedir la concreción del riesgo o reducir sus efectos.

Brück (2005) plantea la existencia de varios tipos de efectos económicos, tanto los directos, los derivados de la pérdida de activos y de producción, robo, fraude, virus informáticos, vidas y otros, como los costes indirectos debidos a las interacciones entre los distintos agentes y políticas como los que Chen y Siems [6] analizan para las respuestas de los mercados de capitales. Conocer el efecto de los riesgos y de las medidas adoptadas es necesario para evitar, por ejemplo, generarse un efecto de "sobreprotección" o, dicho en otras palabras, que las inversiones en ciberseguridad sobrepasen los beneficios que aporta o que una regulación inadecuada disminuya la eficiencia de los mercados.

Aspectos económicos de la ciberseguridad

Uno de los factores que caracteriza el mercado de la ciberseguridad es la falta de competencia. En términos generales, el mercado disciplina a través de los precios y del número de competidores, pero la existencia de grandes proveedores de servicios y operadores en el ciberespacio restringe la competencia. La capacidad de negociación de los usuarios y su poder de mercado es prácticamente inexistente. El poder de monopolio u oligopolio limita, por lo tanto, las posibilidades de que los usuarios puedan cambiar de proveedor, ya que el coste para el consumidor puede ser muy elevado o que puedan exigir niveles de ciberseguridad adecuados[7]. Lo anterior, unido a la necesidad de acelerar el lanzamiento al mercado de nuevos productos, facilita la aparición de brechas de seguridad y de actividades ilícitas cuyos costes se trasladan a los usuarios, sin que éstos repercutan prácticamente en los productores[8]. Esta situación implica la existencia de asimetrías de información entre la oferta y la demanda, de forma que "los proveedores no conocen el alcance real de la seguridad del software y los compradores no están dispuestos a pagar el precio adicional por el software porque no tienen suficiente información sobre su nivel de seguridad" según Fonfría y Duch-Brown[9].

[6] Chen, A.H. y Siems, T.F. (2004) analizan para las respuestas de los mercados de capitales "The Effect of Terrorism on Global Capital Markets". *European Journal of Political Economy.*

[7] Lilian Ablon y otros (2016), "Consumer attitudes toward data breach notifications and loss of personal information", The RAND Corporation.

[8] Ravi Sen (2018), "Challenges to Cybersecurity: Current state of Affairs", *Communications of the Association for Information Systems*, vol. 16 (2).

[9] Antonio Fonfría y Néstor Duch-Brown (2019), "L'Economía de la Ciberseguretat", *Revista Económica de Catalunya* nº 80, p. 74

La cuestión que surge en este punto es, cómo se puede estimular que las empresas realicen más esfuerzos en mejorar la seguridad del software. Obviamente, no es fácil debido a que el coste de las brechas de seguridad que soportan puede ser muy reducido si se compara con el coste individual y, por agregación, el coste social que genera. En realidad, es un problema de asimetría de información, particularmente de riesgo moral[10], según el cual la mayor información que tienen las empresas les permite llevar a cabo comportamientos oportunistas en su beneficio, ya que los usuarios no poseen información suficiente sobre la actividad realizada por la empresa en términos de niveles de seguridad del software. Debido a ello, los usuarios tampoco están dispuestos a pagar un precio adicional por la seguridad, ya que esperan que sean ellas las que aporten soluciones a las brechas que hayan dejado, lo que produce una falta de alineación de objetivos entre las partes.

A ello es necesario unir los problemas de red que se generan cuando algunos usuarios observan que otros sufragan el nivel de seguridad en beneficio del conjunto, lo que resta incentivos para que los que poseen un menor nivel de seguridad mejoren su propia seguridad. Sin embargo, existe un *trade-off* entre eficiencia y resiliencia, de manera que un aumento de la eficiencia a fin de reducir los costes suele ir acompañado de una menor resiliencia por lo que un único fallo de seguridad implicaría un importante efecto cascada[11]. Así, las ganancias de eficiencia en el corto plazo normalmente irán en detrimento de una mayor vulnerabilidad a largo plazo. Es más, tal y como exponen Fonfría y Duch-Brown: “Cuando el agente a cargo de la protección de un sistema de información no es el mismo que sufre los efectos cuando ésta falla, el riesgo de admitir fallos es mayor. Desafortunadamente, la asignación de riesgos en entornos digitales tiende a ser bastante pobre. Como consecuencia, el análisis de ciberseguridad necesariamente debe tener en cuenta los incentivos de las partes interesadas”[12] .

En este sentido, un mercado de derivados seguridad del software podría llevar a los profesionales a un consenso de precios sobre el nivel de seguridad de un producto. De este modo si a una fecha dada no se han encontrado vulnerabilidades sobre un software o se han encontrado y solucionado, su precio de negociación indicaría la opinión de consenso del mercado sobre la seguridad del programa. Por lo tanto, es posible que se puedan utilizar derivados de seguridad del software para cubrir los riesgos de los proveedores de software, jugadores, inversores de empresas de software y compañías de seguros. Los mismos autores han sugerido que las aseguradoras podrían asignar premios basándose en las infraestructuras y los procesos a través de los cuales éstas se gestionan. El problema es que esta posibilidad no se está utilizando de forma amplia debido a que hay problemas de interdependencia de riesgos basada en dos factores. El primero es la interdependencia física de las infraestructuras, ya que se utilizan por varios operadores simultáneamente. Y, el segundo, denominado interdependencia lógica, se

[10] **Allar Dembe y Leslie I. Boden (2020), “Moral Hazard: A Question of Morality?”, *New Solution*, 10 (3), pp. 257-279, febrero de 2020.**

[11] Comisión Europea, “Cybersecurity. Our Digital Anchor. A European Perspective”, Joint Research Centre, junio de 2020.

[12] Fonfría y Duch-Brown, Op. Cit. (2020), p. 77.

refiere a que los ciberataques explotan generalmente la vulnerabilidad de un sistema que se utiliza por numerosas empresas[13].

Como se desprende de las páginas anteriores, el comportamiento de unos agentes posee importantes efectos no esperados o deseados sobre otros, es decir, externalidades, en el ámbito de la ciberseguridad cuyos tres tipos más relevantes serían las siguientes según Duch-Brown[14]. Las externalidades de red vinculadas a la elevada concentración de la industria del software, que suponen que cuanto mayor sea la red, mayor será el valor para cada uno de sus miembros. (en el caso de los protocolos de Internet, la presencia de externalidades de red también explicaría por qué muchas de las actualizaciones seguras han fallado, ya que los beneficios no se materializan hasta que muchos usuarios también lo han adoptado, lo que impide, al menos, limita *de facto* su adopción). En segundo lugar, las externalidades –negativas–, debidas al mayor coste social de ciberseguridad frente al coste individual derivado de su falta. Por último, las externalidades debidas a la interdependencia y que conduce a que las inversiones de unos agentes dependen de su percepción de las inversiones de los demás[15].

El impacto económico de los delitos cibernéticos

La ciberdelincuencia crece de la mano de la digitalización. Los ciberdelincuentes de alto nivel son tan sofisticados como las empresas tecnológicas más avanzadas y, al igual que ellas, han adoptado rápidamente la computación en la nube, la inteligencia artificial, el software como servicio y el cifrado de última generación, entre otros desarrollos tecnológicos recientes. La ciberdelincuencia sigue siendo demasiado fácil, ya que muchos usuarios de tecnología no toman las medidas de protección más básicas y muchos productos tecnológicos carecen de defensas adecuadas, mientras que los ciberdelincuentes utilizan todo tipo de recursos tecnológicos para identificar objetivos, automatizar la creación y entrega de software y la monetización de lo que roban.

Una advertencia importante es que no existe una definición generalmente aceptada de ciberdelincuencia o ciberseguridad, lo que entorpece la recogida de información estadística adecuada. Varios esfuerzos a escala mundial han intentado establecer criterios para determinar la ciberdelincuencia, comparándolos con otros tipos de delincuencia[16]. En estos ejercicios, un elemento relevante reside en la dificultad de monetizar la ciberdelincuencia porque los delincuentes no siempre monetizan todo el valor de lo que han robado y, en particular, en el caso del robo de propiedad intelectual ya que puede distorsionar las estimaciones. A partir de estudios como los citados del CSIS y de trabajos anteriores se ha elaborado una estimación de las pérdidas económicas potenciales asociadas a la ciberdelincuencia, como porcentaje del producto interior bruto (PIB). Para comprobar sus resultados, compararon esta estimación con las

[13] Anderson, Ross (2007), "Incentives and information security", *Algorithimic Game Theory*, Cambridge University Press, cap. 25.

[14] Nestor Duch-Brown (2017), "The Competitive Landscape of Online Platforms", *JRC Digital Economy Working Paper* 2017-04, Joint Research Centre.

[15] Hal Varian (2004), "System Reliability y Free Riding", *Advances in Information Security*, vol 12. Springer.

[16] Notablemente, los realizados por el Centre for Strategic and International Studies (CSIS) de Washington D.C. en sus informes: "The Economic Impact of Cybercrime and Cyber Espionage" de julio de 2013 y "Net Losses: Estimating the Cost of Cybercrime" de junio de 2014.

pérdidas notificadas por los pocos países en los que tenían más confianza en la recogida y notificación de sus datos nacionales. Una primera, y relevante, conclusión es que la ciberdelincuencia no es la actividad ilegal que más pérdidas económicas genera; un honor que ostenta, todavía, la corrupción gubernamental y al que le siguen el tráfico de estupefacientes y la ciberdelincuencia. Sin embargo, si en lugar de considerar las pérdidas económicas, miramos el número de víctimas, entonces la ciberdelincuencia es el líder indiscutible (el Informe del CSIS de 2014 sugiere que dos tercios de las personas en línea, es decir más de dos mil millones de personas, han visto su información personal robada o comprometida. Otra encuesta reveló que el 64% de los estadounidenses habían sido víctimas de acusaciones fraudulentas o de pérdida de información personal[17]. Por su parte, las cifras de Eurostat indican que el 45% de los individuos de la Unión Europea sufrieron algún tipo de ciberataque en 2019[18]. La ciberdelincuencia es una noticia de primera página porque afecta a todos, y porque tiene una elevada rentabilidad: se trata de un delito de bajo riesgo que genera elevados beneficios. Un ciberdelincuente inteligente puede conseguir centenares de miles, incluso millones de euros, sin prácticamente ninguna posibilidad de ser detenido o encarcelado. Si se piensa en los grandes delitos informáticos, hasta la fecha no se ha procesado a ninguno de sus autores. Las fuerzas y cuerpos de seguridad pueden ser competentes a la hora de perseguir a los ciberdelincuentes, pero muchos de éstos simplemente operan fuera de su alcance. Esta es una de las razones por las que el coste de la ciberdelincuencia sigue aumentando. En su Informe de 2014, el CSIS estimó que la ciberdelincuencia cuesta a la economía mundial casi 500 mil millones de dólares, es decir, alrededor del 0,7% de los ingresos mundiales. Esto cifra superaría los valores del PIB de la mayoría de los países del mundo, exceptuando los más grandes, lo que la convierte en una ocupación muy lucrativa. En su Informe de 2018, la misma organización calcula que la ciberdelincuencia puede hoy costar al mundo casi 600 mil millones de dólares, es decir, el 0,8% del PIB mundial.

De acuerdo con el informe del CSIS de 2014, este crecimiento se debe a una rápida adopción de nuevas tecnologías por parte de los ciberdelincuentes; al incremento de nuevos usuarios en línea que provienen de países con escasa cultura de ciberseguridad; al crecimiento de la ciberdelincuencia como servicio y de los “centros” de ciberdelincuencia y, finalmente debido a una creciente sofisticación financiera entre los ciberdelincuentes de alto nivel que, entre otras cosas, facilita la monetización. La monetización de la información obtenida, que siempre había sido un problema para los ciberdelincuentes, parece haber dejado de ser un freno a este tipo de actividades debido a las mejoras en los mercados negros de ciberdelincuencia y al uso de monedas digitales. Los números de tarjetas de crédito robados y la información personal identificable se ponen a la venta en grandes cantidades en la web oscura (“dark web”) utilizando un complejo conjunto de transacciones en las que participan diversos tipos de intermediarios, tanto en mercados legales como en mercados negros. El robo financiero se transfiere a las cuentas bancarias propias de los delincuentes a través de una serie de transferencias destinadas a ocultar y confundir. La propiedad intelectual es utilizada por los adquirentes o vendida. La moneda digital hace que los pagos de los programas de secuestro de archivos sean más fáciles y menos rastreables.

[17] “Americans and Cybersecurity” Pew Research Center, 26/I/2017.

[18] Eurostat, “Security related problems experienced when using the internet”, 15/IV/2020.

La ciberdelincuencia opera a gran escala, lo que provoca que la cantidad de actividades malintencionadas en Internet sea verdaderamente asombrosa. Los proveedores de servicios de internet más grandes indican que por sus redes pasan alrededor de 30 mil millones de escaneos maliciosos al día, como resultado de los esfuerzos automatizados de los ciberdelincuentes para identificar objetivos vulnerables[19]. Muchos investigadores monitorean la cantidad de nuevos programas maliciosos publicados, con estimaciones que oscilan entre 300 mil y un millón de virus y otros productos malintencionados creados diariamente[20]. La mayoría de ellos son scripts automatizados que buscan en la web dispositivos y redes vulnerables. La suplantación de identidad (phishing) sigue siendo la manera más popular y fácil de cometer la ciberdelincuencia.

Las nuevas tecnologías hacen que las personas y las empresas sean más eficientes y eficaces, incluidos los ciberdelincuentes. Éstos adoptan las nuevas tecnologías a un ritmo rápido. El desarrollo de programas maliciosos está automatizado, y cada día se generan miles de piezas nuevas. Como la actividad de Internet se ha trasladado a plataformas móviles, la ciberdelincuencia la ha seguido. El navegador Tor, un producto informático gratuito que permite una actividad de internet anónima e imposible de rastrear, se ha convertido en el medio más usado por los ciberdelincuentes, que evidentemente prefieren operar en la «web oscura». Algunos ciberdelincuentes incluso utilizan herramientas de inteligencia artificial para encontrar objetivos. Por último, bitcoin y otras monedas digitales son, tanto el objeto del robo, como un medio de pago y de transferencia de dinero para los ciberdelincuentes. Al combinar servicios de anonimización y monedas digitales (anonimizadas) con un mercado negro de ciberdelincuencia ya sofisticado –en la forma en que se organizan, en su especialización y en las herramientas de ataque que ofrecen, a menudo diseñadas para evadir las defensas de la red–, se resuelve uno de los principales problemas a los que se enfrentaban los ciberdelincuentes en el pasado: cómo monetizar la información que habían robado.

Además, se espera también un mayor crecimiento de la ciberdelincuencia, ya que los piratas informáticos se aprovecharán del despliegue masivo de los dispositivos del «Internet de las Cosas» (IoT por sus siglas en inglés) mal protegidos que, aunque no son especialmente valiosos, ofrecerán enfoques nuevos y sencillos para robar información personal, acceder a datos o redes valiosos o facilitar ataques de denegación de servicios. La ciberdelincuencia también seguirá creciendo a medida que los piratas informáticos aumenten su uso de herramientas de inteligencia artificial para crear programas maliciosos e identificar objetivos y pasar a la nube. Aprovecharán igualmente los servicios en la nube tanto como objetivos, como en forma de herramientas para albergar programas maliciosos y lanzar ataques.

El fraude, el robo de propiedad intelectual, la denegación de servicios o el secuestro (*ransomeware*) producen gran parte de las pérdidas económicas de la ciberdelincuencia, al igual que los costes de recuperación (limpieza después del delito) y de oportunidad (el lucro cesante debido a la necesidad de gastar más en

[19] "AT&T Sees 30 Billion Malicious Networks Scans Daily", *Security Week*, 15/VI/2020.

[20] Virginia Harrison y Jose Pagliery (2015), "Nearly 1 million new malware threats released every day," *CNN,* 14/IV/2015.

ciberseguridad). Las pérdidas debidas al bloqueo o desviación de los flujos financieros de las empresas suelen ser mayores que las pérdidas económicas, pero ambas son difíciles de cuantificar.

Existe un coste de oportunidad cada vez mayor para las economías nacionales, ya que las personas adoptan comportamientos en línea menos eficientes para evitar la exposición a la ciberdelincuencia. Por ejemplo, y según una encuesta realizada a 40 mil hogares estadounidenses, el 45% indicó que la preocupación por la ciberdelincuencia les impedía realizar transacciones financieras, comprar bienes o servicios o introducir en redes sociales[21]. Según cifras de Eurostat, la proporción de europeos en línea que han visto limitada su actividad debido a consideraciones de ciberseguridad es del 51%[22]. Aunque el coste y el riesgo reales pueden ser bajos, la percepción del riesgo está reconfigurando la manera en que las personas utilizan Internet de forma que perjudican el crecimiento económico.

Sin embargo, la fascinación que generan las tecnologías digitales en todo el mundo y el deseo de utilizarlas hacen que las personas acepten fácilmente los riesgos asociados. Es posible que, a pesar del alud de noticias sobre casos de ciberdelincuencia, las personas, las empresas y los gobiernos estimen que el riesgo y el coste de ser víctima de la ciberdelincuencia son bajos y aceptables. Esto está cambiando, ya que las prácticas empresariales y contables tienen en cuenta el riesgo cibernético. La expansión de la IoT puede aumentar los costes de oportunidad si las personas son reacias a confiar en el futuro, los dispositivos basados en internet, como los utilizados en los dispositivos sanitarios, los hogares inteligentes o los vehículos autónomos.

Una manera de entender el efecto de la ciberdelincuencia es compararla con la economía digital, el segmento de la economía mundial que crece con mayor rapidez. Si atendemos a las cifras proporcionadas por una de las pocas estimaciones que se disponen[23], la economía digital se habría situado en 4,2 billones de dólares en 2016. Utilizando esta cifra, podemos considerar la ciberdelincuencia como un impuesto sobre el crecimiento del 14%. Si la comunidad internacional pudiera ponerse de acuerdo para realizar un esfuerzo concertado y efectivo para reducirlo, los resultados serían beneficiosos para el desarrollo y la prosperidad de todos los países.

Conclusiones y propuestas

Como se ha mencionado anteriormente, la seguridad económica en un elemento que debería formar parte de todo plan de desarrollo económico de los países, pero al que no se le ha prestado suficiente atención. Dada la creciente importancia de la ciberseguridad dentro de la seguridad nacional, esta debe formar parte también de los planes de seguridad económica ya que los costes económicos asociados a la misma son, como hemos podido ver, enormes. En la medida en que la economía digital avance, los riesgos asociados a la ciberseguridad también crecerán si no se toman medidas que

[21] United States Census Bureau, "Data releases", 2014.

[22] Eurostat, "Activities via internet not done because of security economics", 15/IV/2020.

[23] Boston Consulting Group, "The Connected World Report. The Internet Economy in the G-20", marzo de 2020.

los limiten. Una creciente inseguridad en entornos digitales no hará más que limitar la capacidad de crear riqueza y de promover la innovación.

De aquí se desprende la necesidad de una mayor y mejor captación de información y una cooperación internacional más amplia y que progrese a una mayor velocidad. Sin embargo, en el mundo virtual es cada vez más complejo ordenar –y legislar– debido a la aceleración del progreso tecnológico, estos aspectos, lo que sin duda conlleva asociados otros tipos de costes económicos. Esto hace que la ciberdelincuencia forme parte de un problema más amplio, ya que las naciones experimentan una revolución digital que ha cambiado las empresas, la política, la seguridad y la aplicación de la ley. Nuestra capacidad para gobernar esta revolución digital ha quedado obsoleta. La contabilidad es una de las funciones más básicas del gobierno, ya que permite a las naciones adquirir sistemáticamente información que les ayude a gobernar y prestar servicios a los ciudadanos. Una mejor contabilidad de la ciberdelincuencia será esencial para el mundo digital en el que estamos avanzando. Estimar el coste de la ciberdelincuencia puede empezar a ayudar al mundo a gestionar y reducir la ciberdelincuencia, tarea cuya importancia no hará sino aumentar a medida que crece nuestra dependencia de las tecnologías digitales.

Del análisis precedente se desprenden algunas propuestas que no se basan en recomendaciones sobre cómo hacer frente a la ciberdelincuencia, lo cual excede estas páginas, pero si algunos pasos que resultan importantes a partir del estudio de los principales aspectos económicos y de costes realizado. Entre ellas se pueden destacar las siguientes:

- La protección contra la mayoría de los ciberdelitos se consigue mediante la aplicación uniforme de medidas básicas de seguridad (como la actualización periódica y los parches, así como las arquitecturas de seguridad abiertas) y la inversión en tecnologías defensivas, desde los dispositivos hasta la nube. No requiere medidas defensivas más sofisticadas y esta responsabilidad recae principalmente en las empresas y los consumidores.

- La cooperación internacional facilita la lucha contra la ciberdelincuencia, especialmente la de los países que no cuentan con la regulación o las capacidades adecuadas y crean problemas para sus vecinos y la comunidad internacional, pero las agencias nacionales requieren recursos adicionales para desarrollarla.

- Es esencial mejorar la recopilación de información estadística relevante por parte de las autoridades nacionales. Una mayor normalización (datos sobre amenazas) y la coordinación de los requisitos de ciberseguridad mejorarían la seguridad, en particular en sectores clave como el financiero.

Sin este tipo de acciones, la ciberdelincuencia seguirá creciendo a medida que aumente el número de dispositivos conectados y el valor de las actividades en línea. Una mejor recogida de datos sobre ciberdelincuencia es esencial para abordar el problema y justificar la aplicación de recursos adicionales. La recogida de datos puede ser una cuestión políticamente delicada, ya que las víctimas preferirán a menudo no denunciar la ciberdelincuencia. Igualmente puede resultar complejo cuantificar el valor de los

bienes y servicios intangibles y algunos delitos financieros cibernéticos, como por ejemplo la manipulación del mercado de valores, muchos de los cuales son actualmente indetectables. A pesar de toda la atención prestada a la ciberseguridad, su carácter transnacional y la complejidad de la tecnología (que afecta a la recogida de información) dificultan la gestión por parte de cualquier país.