Relanzamiento del Plan de Ciberseguridad de la UE

Javier Alonso Lecuit | Miembro del Grupo de Trabajo sobre Ciberpolítica, Real Instituto Elcano.

Tema

La Comisión Europea ha propuesto al Parlamento y Consejo de Europa un amplio conjunto de medidas para hacer frente a la escalada de ciberamenazas y ciberdelitos que registra la Unión (Cybersecurity Package).

Resumen

Los ciudadanos, empresas y Estados europeos se ven expuestos a nuevos riesgos a medida que la ciberdelincuencia multiplica impunemente la sustracción de datos, los delitos contra la propiedad intelectual y los fraudes, así como los actos de ciberespionaje con fines comerciales o políticos originados desde Rusia, China o Turquía para desestabilizar Estados, instituciones o infraestructuras de la UE. El impacto económico de los ciberdelitos en la UE se ha quintuplicado durante los últimos cuatro años. La preocupación trasciende el daño individual físico o económico, pues la libertad y los derechos civiles de los ciudadanos de los Estados democráticos se ven amenazados por organizaciones y Estados que operan habitualmente desde países externos a la UE, tal como se ha constatado en el curso de los últimos procesos electorales.

En respuesta a esta comprometida situación, la Comisión Europea ha propuesto al Parlamento y Consejo de Europa un amplio conjunto de medidas orientadas a coordinar y reforzar las capacidades de la UE en materia de ciberseguridad. Entre otras, resaltan la creación de una Agencia Europea de Ciberseguridad y la definición de un marco europeo de certificación junto a nuevos instrumentos legislativos. Algunos Estados han mostrado discrepancias sobre la conveniencia de añadir nuevas medidas sin antes haber culminado el anterior plan de ciberseguridad de 2013.

El presente trabajo es un breve análisis crítico del nuevo Plan Estratégico que delimitará el terreno de juego de la ciberseguridad europeo en los próximos años ante la imparable progresión de la ciberdelincuencia en la comisión de delitos y actos terroristas añadido a los retos que ya plantean nuevos paradigmas tales como el Internet de la Cosas (IoT), la digitalización de la industria (Industria 4.0) y la economía digital de los datos.

Análisis

La Comisión Europea ha revisado desde mediados de 2016 con carácter de urgencia el Plan Estratégico de Ciberseguridad de 2013,[1] el desempeño de la *European Union Agency for Network and Information Society* (ENISA)[2] y otros instrumentos europeos en la ciberseguridad y ciberdefensa europea en el contexto de la Estrategia de Mercado Digital Único[3] y la Hoja de ruta de Bratislava.[4]

Esto responde a la creciente preocupación de las entidades públicas y privadas en materia de ciberseguridad, los vacíos operativos y jurídicos que plantean las nuevas tecnologías, así como la limitada eficacia de las acciones no legislativas promovidas hasta la fecha por las Instituciones Europeas, principalmente achacables a la falta de armonización de las actuaciones de los Estados y la fragmentación del mercado.

El 13 de septiembre, el presidente de la Comisión Europea, Jean-Claude Juncker, declaró en el discurso anual sobre el Estado de la Unión que "Europa sigue sin estar adecuadamente equipada para defenderse de los ciberataques". Julian King, comisario de Seguridad de la UE, añadió el 9 de octubre: "Hemos subestimado la escala del cibercrimen". Andrus Ansip, vicepresidente responsable del Mercado Único Digital, indicó: "Ningún país puede hacer frente, por sí solo, a los retos de ciberseguridad. Nuestras iniciativas refuerzan la cooperación de forma que los Estados miembros de la UE puedan acometer juntos estos desafíos".

El relanzamiento del Plan Estratégico de Ciberseguridad Europeo presentando al Parlamento y Consejo el 13 de septiembre de 2017 es un paquete de medidas orientadas a coordinar y reforzar las capacidades de la UE y los Estados en tres planos: (1) el desarrollo de la resiliencia; (2) el refuerzo de la capacidad de respuesta; y (3) la definición de nuevos instrumentos penales.

El desarrollo de la resiliencia

Con el objetivo de desarrollar la resiliencia de la UE en su conjunto y de los Estados individualmente, la Comisión formula la creación de una Agencia de Ciberseguridad Europea con mandato permanente instituida a partir de la actual ENISA. La Comisión ha previsto que la Agencia incremente en cuatro años el actual presupuesto de ENISA de 11 millones de euros a 23 millones y la plantilla de 84 a 125 personas. Las funciones de la nueva agencia se concretan en:

[1] Véase SWD(2017) 295 final, "Assessment of the EU 2013 cybersecurity strategy", 13/IX/2017, https://ec.europa.eu/transparency/regdoc/rep/other/SWD-2017-295-F1-EN-0-0.PDF.

[2] Véanse "Inception impact assessment – Proposal for a Regulation revising ENISA Regulation", https://ec.europa.eu/info/law/better.../090166e5b397d2bd_en; y "Final report on the Evaluation of the European Union Agency for Network and Information Security (ENISA)", 19/IX/2017, https://ec.europa.eu/digital-single-market/en/news/final-report-evaluation-european-union-agency-network-and-information-security-enisa.

[3] Véase http://europa.eu/rapid/press-release_IP-15-4919_en.htm.

[4] Véase http://www.consilium.europa.eu/media/21234/160916-bratislava-declaration-and-roadmap-es.pdf.

(cont.)

- La creación de un marco de certificación y estandarización de ciberseguridad de productos y servicios a escala de la UE.

- La creación del secretariado de la red europea de CSIRT.[5]

- El apoyo a la Comisión y los Estados en la implantación sectorial de la Directiva NIS.

- La ayuda operativa a los Estados para la gestión de incidentes y colaboración para el desarrollo de capacidades a nivel nacional o la concienciación para la prevención de incidentes.

En relación al primer punto, la Comisión tiene el propósito de reducir la actual fragmentación del mercado de ciberseguridad europeo propiciando un esquema armonizado y voluntario para la certificación y estandarización de ciberseguridad de productos *hardware*, *software* o servicios IT, facilitando a usuarios finales, empresas y administraciones públicas una elección informada de los mismos.

Con este objetivo, la Comisión busca simplificar la multiplicidad de esquemas de certificación, reducir costes y barreras administrativas a los proveedores en la UE y promover el concepto de *cybersecurity by design* como ventaja competitiva del producto o servicio. Así, la certificación de un elemento dado será reconocida en la totalidad de los Estados de la UE, mientras que una compañía dada no se verá obligada a solicitar una certificación, en ocasiones distinta, en cada uno de los Estados en los que opere con un mismo producto.

La acreditación proporcionada por cualquiera de las entidades designadas tendrá una validez de cinco años, siendo renovable durante un nuevo período siempre que se cumpla con los requisitos regulatorios. Corresponde a cada Estado designar la autoridad que supervise el cumplimiento del esquema de certificación y resuelva las reclamaciones de la industria en relación al desempeño de las entidades independientes de certificación. Finalmente, la Comisión propone la creación de un Grupo de Certificación Europeo de Ciberseguridad, formado por un representante de las autoridades de certificación de cada Estado, cuya misión será apoyar a la Comisión en el desarrollo de las políticas de certificación, colaborar con la Agencia de Ciberseguridad Europea en el desarrollo de esquemas de certificación y mediar con los organismos de estandarización.

Es importante subrayar que la intención de la Comisión no es redefinir los actuales estándares y certificaciones sino reordenar, armonizar, simplificar y complementar en caso necesario su aplicación en la UE. En este sentido, insta a los Estados a no definir a nivel nacional certificaciones que se solapen a las establecidas a nivel europeo.

[5] *Computer Security Incident Response Team*.

(cont.)

La industria europea de ciberseguridad, representada por la *European Cybersecurity Organisation* (ECS) y el acuerdo de Partenariado Público-Privado (cPPP) [6] desempeñará un papel muy relevante en este proceso. El grupo de trabajo ECS-WG1 *Standardisation, certification, labelling and supply chain management*[7] de ECS aglutina una diversidad de compañías de distintos sectores que cuentan con distintas exigencias regulatorias y que manifiestan a veces posiciones no alineadas. A pesar de ello, el ECS-WG1, cuyo trabajo se encuentra en una fase preliminar, propone establecer un único marco de certificación válido en los distintos sectores[8] de carácter voluntario, dadas las diferentes características y necesidades de cada sector y segmento de negocio.

La ciberdisuasión en refuerzo de las capacidades de respuesta de la UE

La Comisión ha propuesto una estrategia de ciberdisuasión, que se concreta el uso de herramientas tecnológicas de ciberseguridad para proteger los elementos físicos y lógicos junto a cinco líneas de actuación a fin de reforzar la capacidad de respuesta de la UE en su conjunto y de los Estados individualmente:

- Creación en 2018 de un centro europeo de investigación y competencias en materia de ciberseguridad mediante la puesta en marcha de un proyecto piloto para ayudar a desplegar las herramientas y tecnologías, así como el desarrollo de las capacidades a escala nacional y de la UE.

- La Recomendación[9] adoptada el 13 de septiembre de 2013, para la respuesta coordinada ante incidentes de ciberseguridad a gran escala, que establece un plan rector (*the blueprint*) por el que la UE y los Estados miembros cuenten con capacidades de reacción rápidas y coordinadas, mediante la activación de un marco de respuesta común por definir.

- Incluir la ciberdefensa en el Marco de la Cooperación Estructurada Permanente (PESCO) y el Fondo Europeo de Defensa en apoyo de proyectos y consolidar las capacidades de los Estados. Asimismo, la UE creará en 2018 una plataforma de

[6] En el marco de la Estrategia de Ciberseguridad de la UE de 2013, la Comisión Europea y la Organización Europea de Ciberseguridad (ECSO) suscribieron en julio de 2016 un acuerdo de Partenariado Público-Privado (cPPP) con el doble propósito de fomentar la cooperación entre los actores públicos y las empresas europeas en el curso de las primeras etapas del proceso de innovación de productos y servicios de ciberseguridad, así como estimular la industria de ciberseguridad europea, ayudando a alinear la oferta y demanda de usuarios finales, así como sectores que son clientes importantes de soluciones de ciberseguridad (por ejemplo, energía, salud, transporte y finanzas). La UE invertirá hasta 450 millones de euros en proyectos bajo el paraguas de la cPPP en el marco del programa de investigación e innovación Horizonte 2020, cuyo presupuesto total contando con la aportación del sector privado es de 1.800 millones de euros. Véase https://ecs-org.eu/cppp.

[7] Véase https://ecs-org.eu/working-groups/wg1-standardisation-certification-labelling-and-supply-chain-management.

[8] Véase "Cybersecurity partnership: Europe lacks 'strategic' tech muscle", 25/X/2017, http://www.euractiv.com/section/cybersecurity/interview/cybersecurity-partnership-europe-lacks-strategic-tech-muscle/.

[9] Véase "Recomendación y Anexo C(2017) 6100 final de 13/09/2017", http://ec.europa.eu/transparency/regdoc/rep/3/2017/ES/C-2017-6100-F1-ES-MAIN-PART-1.PDF http://ec.europa.eu/transparency/regdoc/rep/3/2017/ES/C-2017-6100-F1-ES-ANNEX-1-PART-1.PDF.

(cont.)

formación para resolver el déficit de competencias en esta materia. La UE y la OTAN fomentarán la cooperación en materia de investigación e innovación sobre ciberdefensa.

- La posibilidad de crear un fondo de respuesta en casos de Emergencia de Ciberseguridad similar, por ejemplo, al Mecanismo de Protección Civil de la UE establecido para incendios forestales o catástrofes naturales.

- Desarrollar la cooperación internacional, endurecer la respuesta diplomática conjunta de la UE y ampliar la cibercapacidad a terceros países para hacer frente común ante ciberamenazas.

Estas líneas de actuación se verán complementadas a instancias del Consejo de Europa[10] con la adopción conjunta de UE con los Estados de una respuesta a nivel diplomático para prevenir y responder ante actividades delictivas en el ciberespacio (*cyber diplomacy toolbox*), entrando de nuevo en un terreno donde la jurisdicción de los estados y su capacidad para establecer sanciones en el ciberespacio[11] son elementos centrales del debate jurídico.

Los nuevos instrumentos penales

La persecución y criminalización de ciberdelitos plantea complejos retos en la aplicación del concepto de jurisdicción y territorialidad ya que éstos se cometen en su mayoría desde sistemas de información emplazados y/o controlados en cualquier país del mundo.

En paralelo a las iniciativas Comunitarias, los Estados desarrollan individualmente procedimientos legales y técnicos que en ocasiones no se encuentran armonizados y que dificultan la intervención transfronteriza de las autoridades, además de obligar a los proveedores de Internet a ejecutar acciones contradictorias entre los distintos países en los que ofrecen sus servicios o que chocan con el cumplimiento de su legislación nacional.

La CE propone dos nuevas Directivas facilitadoras de una respuesta policial y judicial más eficaz para la detección, rastreo, persecución y sanción de ciberdelincuentes:

- La Directiva para la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo.

- La Directiva para el acceso transfronterizo a pruebas electrónicas en el curso de investigaciones criminales (*e-Evidence Directive*).

[10] Véase "Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities (Cyber Diplomacy Toolbox)", 19/VII/2017, http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf.

[11] Véase "The EU Cyber Diplomacy Toolbox: towards a cyber sanctions regime?", 12/VII/, ISS https://www.iss.europa.eu/content/eu-cyber-diplomacy-toolbox-towards-cyber-sanctions-regime.

(cont.)

Estas dos Directivas son el paso siguiente a la Directiva de 2013[12] que estableció unas normas mínimas para la definición de las infracciones penales y las sanciones aplicables en el ámbito de los ataques contra los sistemas de información para facilitar la prevención de estas infracciones y la mejora de la cooperación entre las autoridades. La Comisión indica que su trasposición ha proporcionado una base mínima –aunque insuficiente– entre los Estados en el uso de las definiciones y estándares comunes para la criminalización los ciberataques.

La futura Directiva sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo[13] (tarjetas de crédito y débito, transacciones *online*, pagos con terminales móviles, criptomonedas, etc.) tiene por objeto proporcionar un marco jurídico tecnológicamente neutro y actualizado, eliminando obstáculos operativos que actualmente entorpecen la investigación y la incoación de procedimientos penales. La Directiva plantea establecer la jurisdicción en relación al emplazamiento de los daños causados en cualquiera de los territorios de los Estados, con independencia de la nacionalidad y localización tanto de los atacantes como de los sistemas de información utilizados.

El fraude a través de medios de pago es una amenaza añadida a la seguridad, ya que aporta ingresos a la delincuencia organizada que permiten financiar delitos de terrorismo, tráfico de drogas, trata de personas, etc. Además, provoca importantes pérdidas económicas y debilita la confianza de los consumidores digitales, lo que puede dañar la actividad económica y la participación de las empresas en un Mercado Digital Único. Es previsible que este tipo de fraude aumente al ritmo de crecimiento de la economía digital. Por ejemplo, Europol estima el fraude con tarjetas en 1.440 millones de euros anuales y que las compañías aéreas pierden unos 1.000 millones de euros anuales en el mundo.

En segundo lugar, la Comisión presentará a inicios de 2018 la Directiva *e-Evidence*,[14] que tiene por objeto facilitar el acceso transfronterizo de las autoridades policiales y judiciales a pruebas electrónicas en el curso de investigaciones criminales en respuesta a las dificultades a que se enfrentan éstas en el curso de las investigaciones.

En este contexto, la Comisión ha reconocido tanto la necesidad como la falta de efectividad de medidas voluntarias de colaboración promovidas hasta la fecha; en consecuencia, ha visto la clara necesidad de complementarlas con medidas legislativas que serán objeto de la Directiva *e-evidence*. En los trabajos previos de evaluación de la Directiva,[15] la Comisión apunta varias opciones para afrontar las dificultades legales en

[12] Véase Directiva 2013/40/EU del Parlamento Europeo y del Consejo de 12 de agosto de 2013.

[13] Véase "Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA", http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1505474896206&uri=CONSIL:ST_12181_2017_INIT.

[14] Véase https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/e-evidence_en.

[15] Véase "Non-paper from the Commission services: improving cross-border access to electronic evidence", 8/VI/2017, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/docs/pages/20170522_non-(cont.)

relación a los aspectos de soberanía en el territorio de la UE y reconoce la dificultad de armonizar los distintos marcos legales de los Estados miembros. Así, propone distintas opciones para la gestión de las ordenes y solicitudes entre las autoridades y los proveedores IT establecidos en terceros países a la UE, autorizando a éstos a responder directamente a las autoridades con independencia del país de emplazamiento en la UE, o el acceso directo de las autoridades a pruebas electrónicas sin que medie el proveedor, así como adoptar medidas legislativas con terceros países a través de tratados multilaterales.

A estas dos Directivas se añaden iniciativas para reforzar las capacidades comunes de las autoridades policiales y judiciales entre Estados, tales como el desarrollo de una plataforma segura única para el intercambios de información en la UE, la estandarización de formularios utilizados entre las autoridades judiciales entre Estados, la financiación de la formación de los agentes en estas tecnologías y la asistencia a los Estados en las capacidades de investigar ciberdelitos, dedicando 10,5 millones de euros en el marco del Fondo Interno de Seguridad (ISF). Asimismo, la Comisión contempla potenciar las funciones de Europol y el Centro Europeo de Cibercrimen (EC3).

En el mismo plano de actuación, el Consejo de Interior y Justicia celebrado en diciembre de 2016 solicitó a la Comisión que definiera su posición y acciones sobre el uso del cifrado de servicios, comunicaciones o terminales y otros mecanismos de anonimización con fines criminales. La Comisión es consciente tanto del papel que desempeña el cifrado en la confianza de la economía digital como de las dificultades que plantea a las investigaciones de las fuerzas de seguridad y autoridades judiciales el empleo del cifrado por la delincuencia y organizaciones terroristas.

La Comisión presentó su respuesta en octubre de 2017.[16] Rechaza la regulación del uso de las técnicas de cifrado y la legalización de puertas traseras debido a los riesgos que éstas entrañan a la privacidad y la integridad de los datos en manos de la delincuencia o de estados hostiles. Asimismo, propone la adopción de medidas legislativas contempladas en la futura Directiva *e-evidence*, medidas para cooperación transfronteriza entre autoridades (una plataforma común de comunicación, la estandarización en la EU de formularios para la cooperación judicial, etc.) y medidas de carácter técnico sin por ello prohibir, limitar o debilitar los mecanismos de cifrado.

En el ámbito técnico, Europol y EC3 ofrecerán a las autoridades de los Estados el apoyo técnico para la aplicación de técnicas de descifrado u otras alternativas que faciliten la información cifrada por los sujetos investigados sin por ello exponer al conjunto de los usuarios a riesgos adicionales de seguridad. Asimismo, la Comisión monitorizará el uso del cifrado por las organizaciones criminales en colaboración con EC3, el Centro Europeo de Cibercrimen (EJCN) y Eurojust, alentando la colaboración de las autoridades con la industria, proveedores de comunicaciones y proveedores de Internet,

paper_electronic_evidence_en.pdf; e "Inception impact assessment", 4/VIII/2017, https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2017-3896097_en.

[16] Véase "Eleventh progress report towards an effective and genuine Security Union", 18/X/2017, pp. 8-10, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20171018_eleventh_progress_report_towards_an_effective_and_genuine_security_union_en.pdf.

los programas de formación específicos para fuerzas de seguridad y autoridades judiciales, etc.

Finalmente, la Comisión indica que la cooperación transfronteriza entre las autoridades de los Estados miembros (*law enforcement agency*, LEA) o entre éstas y terceros países se manifiesta lenta e ineficaz a pesar de su gran importancia. La Comisión también señala la necesidad de mejoras en la cooperación entre LEA y proveedores de Internet, generalmente establecidos en EEUU. Para ello, solicita a los proveedores un contacto único con cada Estado, la alineación de los criterios y mecanismos de colaboración de los proveedores de Internet en la entrega de datos, desarrollar con EEUU programas sobre mejores prácticas en la colaboración entre autoridades judiciales, mecanizar con herramientas online el intercambio de información, etc.

Primeras reacciones

Ahora que el plan necesita del respaldo político del Parlamento Europeo y de los gobiernos representados en el Consejo de Europa han surgido las primeras voces críticas desde algunos de los Estados, encabezados por Alemania, que pueden rebajar las expectativas generadas por la Comisión, diluir los cursos de acción y retardar su efectiva aplicación.

Subyacen inquietudes sobre la subsidiaridad y primacía de los Estados en la salvaguarda de su seguridad, aspectos de armonización con la legislación en curso o debates no resueltos sobre la soberanía y jurisprudencia del ciberespacio.

Para Alemania es prioritaria la efectiva implantación de los mecanismos previos acordados desde 2013, en particular sobre la Directiva NIS. Roland Hartmann, jefe de relaciones internacionales en la Oficina Federal Alemana para la Seguridad de la Información (BSI), declaró a principios de octubre:[17] “lo primero es lo primero... no debemos descuidar que en primer lugar hemos de establecer, tal como me gustaría llamarlo, ‘las habilidades básicas de lectura y escritura en Europa’, así indica la directiva NIS, antes de aspirar a un nivel avanzado de matemáticas, tal como se pretende en el paquete de ciberseguridad”. El representante del BSI también redujo las expectativas de crecimiento en competencias y presupuesto de ENISA (futura Agencia de Ciberseguridad Europea), indicando que éstas no deben sustituir los esfuerzos a nivel nacional, siendo los Estados quienes desplieguen sus propias capacidades, competencias e inversiones. A juzgar por el representante alemán, la implantación de la Directiva NIS en 2018 habrá de fortalecer la confianza y colaboración efectiva entre el sector privado y el Estado en un marco de colaboración público-privada, más allá del mero cumplimiento de las obligaciones regladas.

En la misma línea, el responsable del Servicio de Información Alemán (*Bundesnachrichtendienst*, BND) Bruno Kahl, señaló en una audiencia pública del Comité de Supervisión de Inteligencia Exterior del Bundestag el 5 de octubre el rechazo del BND a la creación de un servicio de inteligencia de la UE que: “La inteligencia está mejor organizada al nivel nacional… yo también estoy en contra de crear tal institución.

[17] Conferencia de ciberseguridad CYBERSEC FORUM, 10/X/2017, Cracovia.

En caso de hacerlo, crearíamos estructuras burocráticas dobles, tanto a nivel europeo como doméstico. Esto reduciría significativamente nuestra eficiencia". Al tiempo, solicitaba en la misma intervención la extensión extraterritorial de la cobertura legal del Estado para la interceptación y bloqueo de contenidos y terminales en un contexto de lucha internacional antiterrorista.

En el ámbito de la estandarización y la certificación, la atribución propuesta a la actual ENISA ha tensionado a organismos técnicos de estandarización como el *European Telecommunications Standards Institute* (ETSI), cuyas especificaciones adquieren rango de norma en los Estados de la Unión. El comité técnico TC-CYBER del ETSI[18] ha declarado recientemente que no existen lagunas en la adecuación de los estándares sobre ciberseguridad a la legislación sino más bien una excesiva profusión e inadecuación de los mismos, añadiendo que es poco efectivo, costoso o incluso contraproducente ofrecer esquemas de certificación "unilaterales y estáticos" que puedan dar a los usuarios un falso sentido de seguridad. Desde la perspectiva del ETSI es necesaria una labor de ordenación e incluso eliminación selectiva de algunos estándares. Es significativa la ausencia de referencias al ETSI en la propuesta de la Comisión Europea (*Cybersecurity Act*).

Conclusión

Una vez pasado el tamiz del Parlamento y Consejo de Europa, corresponde a los Estados iniciar su ejecución, al tiempo que el sector privado, de la mano de sus gobiernos, afronta a mediados de 2016 la recta final para la entrada en vigor de dos regulaciones clave en materia de seguridad: la transposición de la Directiva NIS y el reglamento general para la protección de datos de carácter personal (GDPR).

Mientras tanto, esta batería de medidas de 2017 necesitará de los mismos ingredientes básicos a los empleados en el anterior plan estratégico de ciberseguridad de 2013: la estrecha confianza, firme decisión y cooperación entre los Estados, una sólida colaboración público-privada, la participación de la industria, y recursos, formación y concienciación de los usuarios, entre otros.

Preocupa que la superposición de las múltiples iniciativas pueda dispersar la atención, recursos y prioridades de los protagonistas –empresas y Estados de la UE– en el curso de su ejecución, restando así agilidad y efectividad. Será necesario un importante esfuerzo de praxis para alcanzar en tiempo y forma los objetivos establecidos al ritmo con que la tecnología plantea nuevos retos en materia de ciberseguridad.

Durante los próximos meses, el gobierno, las fuerzas de seguridad y las autoridades judiciales españolas, con la colaboración del sector privado, habrán de evaluar, coordinar y, tras su aprobación, poner en práctica estas nuevas iniciativas en materia de ciberseguridad.

[18] Véase ETSI TC-CYBER, septiembre de 2017, https://www.enisa.europa.eu/events/enisa-cscg-2017/presentations/brookson y http://www.etsi.org/technologies-clusters/technologies/cyber-security.