Dictamen del Comité Económico y Social Europeo sobre la Comunicación Conjunta al Parlamento Europeo y al Consejo: «Política de ciberdefensa de la UE»

(Dictamen de iniciativa)

(2023/C 293/04)

Ponente: **Anastasis YIAPANIS**

Coponente: **Alberto MAZZOLA**

Decisión de la Asamblea	20.9.2022
Base jurídica	Artículo 52, apartado 2, del Reglamento interno
	Dictamen de iniciativa
Sección competente	Comisión Consultiva de las Transformaciones Industriales (CCMI)
Aprobado en sección	27.3.2023
Aprobado en el pleno	14.6.2023
Pleno n.º	579
Resultado de la votación	
(a favor/en contra/abstenciones)	208/1/2

1. **Conclusiones y recomendaciones**

1.1. El Comité Económico y Social Europeo (CESE) apoya la propuesta de política de ciberdefensa de la UE, pero habría esperado que se concediera a la sociedad civil organizada un papel más destacado en el desarrollo de estas propuestas. El Comité considera difícil evaluar en este momento si las futuras iniciativas esbozadas en la Comunicación conjunta se aplicarán y alcanzarán los resultados previstos. Insta a las instituciones de la UE y a los Estados miembros a que den prioridad y hagan avanzar rápidamente las iniciativas anunciadas.

1.2. El CESE hace hincapié en la necesidad de adoptar medidas adicionales para mejorar la capacidad de la UE para detectar ciberamenazas y pide que se destinen fondos a I+D para desarrollar capacidades de vanguardia en la UE. La cooperación entre los sectores público y privado es esencial y no debe ser unidireccional. El CESE considera que es necesaria la coordinación de la UE para abordar la fragmentación y garantizar la cooperación y la inversión conjunta entre los Estados miembros.

1.3. El CESE apoya la creación del Centro de Coordinación de la Ciberdefensa de la UE y recomienda que los Estados miembros se comprometan a proporcionar una respuesta rápida 24/7, evalúen la preparación en materia de ciberseguridad y el rendimiento de los mecanismos de respuesta a las cibercrisis de la UE, centrándose tanto en las capacidades militares como en los sectores críticos identificados en la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo ([1]) (Directiva SRI 2). El Comité respalda que se amplíe el mandato del Centro Europeo de Competencia en Ciberseguridad (ECCC, por sus siglas en inglés) para contribuir a la labor del Centro de Coordinación de la Ciberdefensa de la UE.

1.4. Para mejorar la autonomía estratégica y la soberanía de la UE en materia de ciberseguridad, el CESE considera que desde el sector privado debe desarrollarse o adoptarse una plataforma dinámica de pruebas e intercambio de información en tiempo real, con el fin de identificar el déficit actual de nuestras capacidades existentes. También puede utilizarse para compartir las mejores prácticas, denunciar incidentes de ciberseguridad y crear una lista de la UE de todos los ciberdelincuentes.

([1]) 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 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2) (DO L 333 de 27.12.2022).

1.5. El CESE destaca la necesidad de una mejor preparación frente a los ciberataques, como los rusos en Ucrania, dirigidos en particular a infraestructuras críticas. La cooperación entre los ecosistemas civiles y militares es crucial para la gestión eficiente de las crisis, para la interoperabilidad y para evitar la duplicación de esfuerzos e inversiones, incluso a través de la simulación de ciberataques de prueba.

1.6. El CESE considera que las inversiones en ciberdefensa deben dar prioridad a la protección de la ciudadanía y las infraestructuras críticas de la UE, también mediante el uso de proveedores de equipos y programas informáticos de confianza. Insiste en que se actualicen oportunamente las prioridades y la inversión, que deberán acordarse entre la UE y los Estados miembros, con la participación de las partes interesadas privadas pertinentes.

1.7. La UE debe conservar y desarrollar las capacidades necesarias para garantizar su economía digital, su sociedad, su democracia y sus tecnologías críticas, así como para prestar servicios clave de ciberseguridad. Para garantizar la autonomía estratégica de la UE, es fundamental que se reduzca la dependencia de terceros países. El CESE considera esencial que la UE adopte un enfoque a medio plazo hacia la autonomía por lo que respecta a las tecnologías clave, y aboga firmemente por que las empresas con sede en la UE creen instalaciones de investigación y producción, con una política industrial europea adecuada centrada en un ecosistema de la ciberseguridad autónomo.

1.8. Las pymes deben recibir apoyo específico y tener acceso a programas de financiación que aumenten su resiliencia frente a los ciberataques, así como a oportunidades de asistencia, formación y educación sobre los riesgos de ciberseguridad y cómo protegerse contra ellos. La UE debe proporcionar un mecanismo de incentivos que promueva la familiarización progresiva de las pymes y el desarrollo de pymes innovadoras.

1.9. El CESE apoya el plan para crear una Academia de Cibercapacidades, y pide a la Comisión Europea que coordine y financie programas de formación y formación profesional a gran escala en los que participen todos los Estados miembros y cuyo objetivo sea crear mano de obra cualificada para todas las agencias y organizaciones que participan en la ciberdefensa, así como para las redes civiles privadas.

1.10. El Comité considera que es crucial sensibilizar a los ciudadanos sobre la ciberseguridad para reducir la exposición a ciberataques, y pide que se elaboren planes de estudios educativos en materia de ciberseguridad y programas de formación a lo largo de toda la vida orientados a mejorar las cibercapacidades y el conocimiento. El CESE apoya que la ciberseguridad se integre en todas las futuras políticas públicas de la UE y que se informe al público en general sobre las ciberamenazas.

1.11. El CESE considera que una estrecha cooperación con los aliados de la OTAN en ámbitos militares debe centrarse en la plena coordinación y reciprocidad, proyectos conjuntos de I+D+i, el intercambio de mejores prácticas, amplios programas de formación y simulaciones de ciberataques, con el objetivo principal de ampliar la capacidad de respuesta común.

1.12. El Comité pide al Alto Representante que examine los actuales diálogos bilaterales sobre ciberseguridad y que inicie debates adicionales con otros países y organizaciones internacionales pertinentes con vistas a establecer un marco mundial para la adhesión al Derecho internacional en el ciberespacio, haciendo especial hincapié en la reciprocidad. El Comité considera que la UE está en condiciones de asumir el liderazgo en los debates internacionales sobre el futuro de la ciberseguridad, en particular en el seno de las Naciones Unidas, ya que cuenta con una base sólida de libertades democráticas fundamentales.

1.13. La UE debe adoptar una postura firme contra cualquier tipo de sistema de puntuación ciudadana que vaya en contra de los ciudadanos. El CESE deja claro que la verdadera democracia no puede existir sin una protección eficaz de los datos personales y considera que una gestión responsable y eficiente de los datos es esencial para convertir la hiperconectividad en una ventaja competitiva.

2. **Introducción y observaciones generales**

2.1. La expansión digital de las sociedades va acompañada de un gran número de amenazas a la ciberseguridad generadas por las mejoras tecnológicas. En los últimos años, los ciberataques han aumentado significativamente en número y sofisticación, lo que ha socavado la seguridad de las entidades públicas y privadas. Independientemente de que se trate de programas de secuestro, programas maliciosos, ataques por correo electrónico, violaciones de la seguridad de los datos, desinformación, ataques distribuidos de denegación de servicio u otras formas de ataques, todos ellos suponen una amenaza constante y continua para la seguridad de la UE en su conjunto.

2.2. El CESE acoge favorablemente la *Comunicación conjunta — Política de ciberdefensa de la UE* ([2]) y considera que ha llegado el momento de actuar, con urgencia y de manera coordinada a escala de la UE, con la participación de los ecosistemas tanto civiles como militares del ciberespacio y garantizando un marco de inversión adecuado para las capacidades de ciberdefensa. No obstante, el Comité observa que la Comunicación se limita a declarar la determinación de actuar y a enumerar una lista de futuras iniciativas de la UE que deben materializarse, y considera que es imposible evaluar si estos futuros compromisos se materializarán en realidad, ya que las futuras negociaciones entre los colegisladores influirán naturalmente en el resultado final del plan de acción de la UE en materia de ciberseguridad.

2.3. El ataque ruso a la red de satélites KA-SAT, que perturbó la comunicación entre las fuerzas militares ucranianas y el reciente escándalo que supuso la contratación de Éric Léandri por parte de algunas empresas de defensa para hacer ciberespionaje en su nombre, sitúa la ciberseguridad en el primer puesto de la lista de amenazas para la seguridad en la UE. Si bien el RGPD es un acto legislativo sólido de la UE y lleva en vigor varios años, está claro que la creciente cantidad de datos disponibles es vulnerable y que el riesgo de que terceros crucen el límite de legalidad es cada día mayor.

2.4. Dado el carácter transnacional de los ciberataques, es necesaria una coordinación de la UE para reducir la fragmentación actual y garantizar que los Estados miembros estén preparados para cooperar e invertir conjuntamente. Esto es especialmente importante en el caso de futuros casos en los que un Estado miembro pudiera ser objeto de un ataque y todos los demás deberían poder prestarle apoyo inmediato.

3. **Actuar juntos para una mejor ciberdefensa**

3.1. El Comité toma nota de las ambiciosas iniciativas anunciadas para crear un Centro de Coordinación de la Ciberdefensa de la UE, desarrollar el proyecto CyDEf-X, crear equipos de respuesta telemática rápida, desarrollar una Iniciativa de Cibersolidaridad de la UE y explorar el desarrollo de esquemas de certificación de la ciberseguridad para productos, servicios y procesos TIC. El CESE recomienda que todos los Estados miembros se comprometan a estar preparados para proporcionar una respuesta rápida 24/7, con la participación del Centro de Coordinación de la UE en la evaluación y elaboración de informes periódicos sobre la preparación en materia de ciberseguridad de los Estados miembros y la eficacia del mecanismo europeo de respuesta a las cibercrisis, poniendo el foco tanto en las capacidades militares como en los sectores críticos identificados en la Directiva SRI 2. Cada Estado miembro debe contar con especialistas formados específicamente para intervenir en caso de incidentes de ciberseguridad, y poner a prueba periódicamente su capacidad de intervención en otros Estados miembros.

3.2. Si bien la Comunicación ofrece una larga lista de mejoras paso a paso, el CESE habría esperado encontrar una hoja de ruta explícita sobre la aplicación de estas iniciativas, con una gobernanza y unos plazos de presentación y aprobación claros. Además, el Comité habría esperado que se concediera a la sociedad civil organizada un papel más destacado en el desarrollo de estas propuestas.

3.3. El CESE considera que los Estados miembros deben reforzar su capacidad interna para contrarrestar las ciberamenazas al tiempo que participan en proyectos de cooperación y comparten información y mejores prácticas con sus homólogos de otros Estados miembros. Es necesario invertir rápidamente en capacidades de ciberdefensa y en un despliegue acelerado de tecnologías ([3]) en todos los Estados miembros, así como en la preparación común para detectar ciberataques, defenderse y recuperarse de ellos. Con el fin de apoyar la autonomía de la UE en materia de ciberseguridad, el Comité considera que desde el sector privado debe desarrollarse o adoptarse una plataforma dinámica de pruebas e intercambio de información en tiempo real, centrada en identificar el actual déficit de capacidades.

3.4. El CESE comparte la opinión de que, en este punto, las operaciones militares en el ciberespacio deben seguir siendo estrictamente competencia de los Estados miembros; el Comité apoya la anunciada cooperación entre los equipos militares de respuesta a emergencias informáticas de la UE (milCERT), los equipos de respuesta a incidentes de seguridad informática (CSIRT) y el equipo de respuesta a emergencias informáticas de las instituciones, órganos y organismos de la UE (CERT-UE).

3.5. La Directiva SRI 2 recientemente adoptada y la Directiva relativa a la resiliencia de las entidades críticas (REC) ([4]) ya establecen obligaciones nacionales y sectoriales específicas para el marco de ciberdefensa de la UE. Se requieren nuevas medidas para mejorar la capacidad de detección colectiva de la UE, y el CESE pide que se invierta en I+D para desarrollar capacidades de vanguardia en la Unión.

([2]) Comunicación conjunta — Política de ciberdefensa de la UE.
([3]) Por ejemplo, el Acelerador de Innovación de Defensa para el Atlántico Norte (DIANA, por sus siglas en inglés).
([4]) Directiva REC.

4. **Asegurar el ecosistema de defensa de la UE**

4.1. El CESE considera que las complejidades inherentes y la rápida evolución de los retos tecnológicos han transformado el ecosistema de la defensa y que la ciberseguridad se ha convertido en un asunto común tanto para los sectores militar y civil como para la ciudadanía de la UE. La cooperación entre los ecosistemas civiles y militares es ahora más importante que nunca y debe aportar beneficios en términos de una gestión de crisis más eficaz, así como un progreso continuo y la interoperabilidad, evitando duplicar o multiplicar los mismos esfuerzos e inversiones. Los Estados miembros deben estar preparados para llevar a cabo pruebas de resistencia en las infraestructuras críticas nacionales con el fin de evaluar y aumentar la resiliencia frente a futuros ciberataques.

4.2. El CESE considera que las inversiones en ciberdefensa deben destinarse de manera prioritaria a la protección de los ciudadanos y las infraestructuras críticas de la UE. Dado el rápido ritmo de la transformación digital y la rápida evolución del panorama de amenazas, el Comité insta encarecidamente a que la UE y los Estados miembros acuerden actualizaciones oportunas de las prioridades y la inversión, previa consulta exhaustiva a las partes interesadas del sector privado pertinentes. A menudo, los dispositivos internet de las cosas (IdC) no están tan protegidos como los dispositivos tradicionales, y el CESE pide que se garantice un nivel mínimo de seguridad a través de las plataformas de servicios de gestión de identidad y acceso (IDAM por sus siglas en inglés). Asimismo, dado que la certificación constituye un método clave para ofrecer un mayor nivel de seguridad, el Comité pide que el nuevo enfoque de certificación de la UE haga más hincapié en la seguridad de la IdC.

4.3. La UE debe reforzar la resiliencia frente a los ciberataques y crear una ciberdisuasión eficaz. Las infraestructuras críticas deben estar protegidas contra todo tipo de ciberataques, incluidos los de los sistemas de defensa de la UE. El Comité considera que redunda en el interés estratégico de la UE garantizar que esta conserve y desarrolle las capacidades esenciales para garantizar su economía digital, su sociedad y su democracia, y alcanzar la plena soberanía digital como única forma de proteger las tecnologías críticas y prestar servicios clave de ciberseguridad eficaces. Reducir la dependencia de terceros países también es vital para la autonomía estratégica de la UE. El CESE considera que las agencias sectoriales de la UE (ENISA, AESA, AFE, EMEA, ABE, AES, HADEA, etc.) deberían participar en el proceso y proporcionar orientación en el desarrollo de esquemas de ciberseguridad.

4.4. La pandemia de Covid-19 ha acelerado la transición digital y ha transformado el trabajo tradicional en híbrido o remoto, creando nuevas relaciones y expectativas de trabajo, así como una nueva clase de nómadas digitales, cuyo número está aumentando. El CESE toma nota de los rápidos cambios en el mercado laboral, que han generado la adopción de la arquitectura de «confianza cero» por parte de las empresas, a través de soluciones de gestión de identidad y acceso (IAM) y gestión de accesos privilegiados (PAM). El Comité considera que este tipo de gestión de los recursos de las empresas aporta nuevas soluciones relacionadas con las ciberamenazas y considera que debe apoyarse al sector privado para reforzar el nivel de seguridad de sus soluciones digitales innovadoras.

4.5. El CESE está bastante decepcionado por la afirmación de la Comisión de que «podría establecerse un plan de aplicación en cooperación con los Estados miembros» y considera que dicho plan de aplicación es obligatorio. Considera que debería elaborarse conjuntamente con los Estados miembros y ejecutarse lo antes posible. El Comité expresa su preocupación por la postura de baja injerencia adoptada por la Comisión, e insta a las instituciones de la UE y a los Estados miembros a que faciliten un rápido avance en las iniciativas anunciadas.

5. **Invertir en capacidades de ciberdefensa**

5.1. A medida que avanza rápidamente el desarrollo tecnológico, el ciberespacio se ha convertido en el escenario más reciente de la guerra, después de la tierra, el mar, el aire y el espacio. También ha generado grandes oportunidades de delincuencia para los ciberagentes malintencionados, desde piratas informáticos independientes hasta delincuentes profesionales e incluso agentes estatales.

5.2. La inversión en I+D es vital y el CESE acoge con satisfacción los fondos específicos existentes en el marco del programa Europa Digital, el Fondo Europeo de Defensa, Horizonte Europa y los planes nacionales de recuperación. No obstante, el Comité agradecería más proyectos transnacionales centrados en la cooperación y la interoperabilidad entre los sistemas de ciberdefensa de todos los Estados miembros, así como más sinergias entre los instrumentos de financiación, en particular para respaldar a las pymes innovadoras.

5.3. Tal como se anunció en la Estrategia de Ciberseguridad de la UE en 2020, el Comité observa que el plazo para crear la unidad informática conjunta finaliza este año y está a la espera de noticias sobre la finalización del proceso y la preparación de la UE para responder ante incidentes de ciberseguridad a gran escala. El CESE espera que mejore el conocimiento de la situación de la UE y la capacidad general de respuesta y recuperación.

5.4. El CESE apoya la ampliación del mandato del ECCC para apoyar la actividad del Centro de Coordinación de la Ciberdefensa de la UE. Además, esta red podría promover la soberanía digital europea mediante el desarrollo de una base industrial europea competitiva para las capacidades tecnológicas clave, basada en parte en el trabajo desarrollado por alianzas público-privadas contractuales (APP). Las APP han demostrado ser el enfoque más eficaz para mejorar la ciberseguridad de todo el ecosistema digital, pero no pueden ser unidireccionales: las instituciones públicas también deben compartir su inteligencia con el sector privado.

5.5. El CESE señala que, para hacer frente a los futuros intentos de piratería informática procedentes de ordenadores cuánticos, la UE debe invertir inmediatamente en tecnologías punteras como la criptografía postcuántica. Considera indispensable que Europa adopte un enfoque de autonomía a medio plazo y aboga firmemente por que las empresas con sede en la UE desarrollen instalaciones de investigación y producción. El CESE considera que es importante incrementar los recursos de la UE para la I+i digital y promover la inversión de operadores y proveedores en nuevas funcionalidades técnicas de seguridad, también en relación con nuevas tendencias como la realidad aumentada y el metaverso. En particular, es esencial crear una infraestructura europea distribuida en la nube basada en normas europeas sobre asuntos como el almacenamiento y el tratamiento de los datos ([5]).

5.6. Las pymes deben recibir una atención específica y tener acceso a programas de financiación que mejoren su preparación frente a los ciberataques, así como a programas de asistencia, formación y educación que les ayuden a conocer los riesgos de ciberseguridad y cómo protegerse. La UE debe proporcionar un mecanismo de incentivos que promueva la familiarización progresiva de las pymes.

5.7. La Comisión estima que el actual déficit de capacidades en ciberseguridad asciende a medio millón de personas, y el CESE valora positivamente la propuesta de crear una Academia de Cibercapacidades. Es evidente que los esfuerzos a nivel de los Estados miembros no bastan para reducir el déficit de capacidades, por lo que el Comité propone que, junto con la puesta en marcha de la Academia, la Comisión aproveche el impulso que brinda el Año Europeo de las Competencias y coordine y financie programas de formación a gran escala y programas de EFP a escala de la UE en los que participen todos los Estados miembros y se centren en ofrecer mano de obra cualificada a todas las agencias y organismos que participan en la ciberdefensa, así como a las redes civiles privadas. Debe hacerse especial hincapié en la formación de la mano de obra, en particular en los ámbitos de ciencia, tecnología, ingeniería y matemática (CTIM).

5.8. Además, el CESE considera que es fundamental sensibilizar a los ciudadanos sobre la ciberseguridad con el fin de reducir la exposición a ciberataques, especialmente en lo que respecta a los ciberdelitos básicos contra la población en general. El Comité pide que se elaboren planes de estudios educativos en materia de ciberseguridad y programas de formación en ciberseguridad a lo largo de toda la vida orientados a mejorar las cibercompetencias y hacer que la ciberseguridad resulte más familiar y atractiva para los ciudadanos, especialmente para las generaciones más jóvenes. El CESE está a favor de integrar las reflexiones sobre ciberseguridad en todas las futuras políticas públicas de la UE, así como de informar al público en general sobre las ciberamenazas, en particular a través de programas de formación gratuitos para toda la población, aplicaciones gratuitas de información para teléfonos móviles o mediante acciones de comunicación durante los horarios de televisión de máxima audiencia. En paralelo a estas acciones, debe promoverse un avance cultural generalizado en todos los niveles de la sociedad hacia un enfoque «orientado hacia la ciberseguridad».

5.9. El CESE considera imprescindible garantizar las evaluaciones del perfil de riesgo de los proveedores y aplicar restricciones pertinentes a los considerados de alto riesgo, incluidas las prohibiciones necesarias de los activos y aplicaciones clave considerados críticos y sensibles en una evaluación de riesgos coordinada a escala de la UE, así como la certificación de los proveedores de equipos y programas informáticos de confianza.

6. **La asociación como forma de afrontar los retos comunes**

6.1. El nivel de preparación para futuros ciberataques difiere considerablemente de un Estado miembro a otro. El CESE considera que el primer paso inmediato es crear una plataforma de comunicación de mejores prácticas dentro de la UE, en la que los Estados miembros más avanzados en ciberseguridad puedan compartir sus conocimientos con el resto de países y facilitar su adopción inmediata. Esto ayudaría a mejorar la confianza mutua entre las entidades nacionales. En segundo lugar, el Comité considera que es necesaria una mayor cooperación entre los agentes estatales y no estatales en toda la UE para mejorar la ciberseguridad de los productos y servicios en el mercado interior. El CESE también propone la creación de una plataforma común de la UE para la denuncia de incidentes de ciberseguridad, incluida una lista negra de la UE de todos los activistas de la ciberdelincuencia.

([5]) Como Gaia-X, la iniciativa franco-alemana.

6.2. El CESE considera que la estrecha cooperación con nuestros aliados de la OTAN en el ámbito militar debe centrarse no solo en el desarrollo de capacidades y la detección precoz, sino también en proyectos conjuntos de I+D+i, el intercambio de mejores prácticas y los intercambios entre expertos, amplios programas de formación y simulaciones de ciberataques. El principal objetivo debe ser ampliar la capacidad de respuesta común y crear sinergias para contrarrestar futuras amenazas híbridas, a raíz de las Declaraciones conjuntas de Varsovia de 2016 y de Bruselas de 2018. La cooperación entre la UE y la OTAN aún tiene una serie de vías que pueden aprovecharse, y el progreso inmediato puede marcar una verdadera diferencia a la hora de garantizar la seguridad de nuestros ciudadanos y sociedades.

6.3. El Comité considera que los debates a escala mundial y con nuestros socios internacionales deberían sentar las bases para promover un ciberespacio global y abierto que proteja los derechos humanos, las libertades fundamentales y el Estado de Derecho, y que se centre en el desarrollo de normas internacionales vinculantes en sectores con un rápido desarrollo digital. El CESE aconseja al Alto Representante que revise los ciberdiálogos bilaterales existentes y emprenda nuevas negociaciones con otros países y organizaciones internacionales pertinentes con el fin de promover un marco mundial para la aplicación del Derecho internacional en el ciberespacio, sobre la base de una estricta condición de reciprocidad.

6.4. Por último, el Comité considera que la UE está en las mejores condiciones para liderar los debates internacionales sobre el futuro de la ciberseguridad, especialmente en el marco de los debates de las Naciones Unidas, debido a su sólida base de libertades democráticas fundamentales. La UE también debe comprometerse en la lucha contra los regímenes totalitarios que controlan los datos de los ciudadanos y vulneran sus derechos y libertades, y debe posicionarse firmemente contra cualquier tipo de sistema de puntuación social contra los ciudadanos. El CESE afirma claramente que no puede haber una verdadera democracia sin una protección eficaz de los datos personales, y considera que una gestión responsable y eficiente de los datos es vital para convertir la hiperconectividad en un activo.

Bruselas, 14 de junio de 2023.

El Presidente
del Comité Económico y Social Europeo
Oliver RÖPKE