Consejo de la Unión Europea

Bruselas, 10 de diciembre de 2019
(OR. en)

14972/19

HYBRID 56	**EDUC 478**
DISINFO 18	**AUDIO 118**
AG 68	**DIGIT 179**
PE 257	**INF 332**
DATAPROTECT 300	**COSI 252**
JAI 1307	**CSDP/PSDC 575**
CYBER 328	**COPS 360**
JAIEX 177	**POLMIL 129**
FREMP 176	**IPCR 23**
RELEX 1147	**PROCIV 100**
CULT 141	**CSC 294**

RESULTADO DE LOS TRABAJOS

De:	Secretaría General del Consejo
A:	Delegaciones
Asunto:	Acciones complementarias para aumentar la resiliencia y luchar contra las amenazas híbridas - Conclusiones del Consejo (10 de diciembre de 2019)

Adjunto se remite a las delegaciones las Conclusiones del Consejo sobre las acciones complementarias para aumentar la resiliencia y luchar las amenazas híbridas, adoptadas en la sesión n.º 3739 del Consejo, el 10 de diciembre de 2019.

ANEXO

Conclusiones del Consejo sobre las acciones complementarias para aumentar la resiliencia y luchar contra las amenazas híbridas

1. El Consejo recuerda las Conclusiones del Consejo Europeo[1] y del Consejo[2] pertinentes y reitera su compromiso de reforzar la resiliencia de la Unión y de sus Estados miembros frente a las amenazas híbridas, que son polifacéticas y están en constante evolución, y de mejorar la cooperación para detectarlas, evitarlas y luchar contra ellas.

2. El Consejo reconoce los avances obtenidos en la aplicación del Marco común de lucha contra las amenazas híbridas (2016) y de la Comunicación conjunta sobre el incremento de la resiliencia y el refuerzo de capacidades para hacer frente a las amenazas híbridas (2018), así como el Plan de Acción contra la Desinformación (2018), en consonancia con las Conclusiones del Consejo pertinentes.

3. La responsabilidad de luchar contra las amenazas híbridas incumbe principalmente a los Estados miembros. Los esfuerzos a escala de la UE son de naturaleza complementaria y se llevan a cabo sin perjuicio de la responsabilidad exclusiva de los Estados miembros en cuestiones de seguridad nacional. La lucha contra las amenazas híbridas requiere un planteamiento global en el que se involucren todo el gobierno y toda la sociedad, y en el que se trabaje de manera más estratégica, coordinada y coherente en todos los sectores de actuación pertinentes. Es importante seguir un planteamiento en el que se involucre todo el gobierno y aplicarlo también a escala de la UE.

4. En estas Conclusiones, el Consejo fija prioridades relativas a la protección de nuestras sociedades, ciudadanía y libertades, así como de la seguridad de nuestra Unión frente a amenazas híbridas en el contexto de la aplicación de la nueva Agenda Estratégica para 2019-2024. Para ello, promueve un enfoque exhaustivo en torno a la seguridad, que abarca una mejora de la coordinación, los recursos y las capacidades tecnológicas, partiendo de la importante labor ya completada en diversos sectores de actuación, entre ellos la cooperación en materia de seguridad y defensa de la UE.

---

[1] Concretamente, las Conclusiones del Consejo Europeo de junio de 2019, marzo de 2019, diciembre de 2018, octubre de 2018, junio de 2018, marzo de 2018, junio de 2015 y marzo de 2015

[2] Concretamente, ST 10048/19, ST 6573/1/19 REV1, ST 10255/19, ST 12836/19, ST 7928/16

5. Los esfuerzos por proteger nuestras instituciones frente a las amenazas híbridas deben respetar siempre los derechos fundamentales, entre los que se encuentran la protección de los datos personales, la libertad de expresión e información y la libertad de asociación, consagrados en la Carta de los Derechos Fundamentales.

6. La UE y sus Estados miembros deben seguir desarrollando, formando y ejerciendo las capacidades de detección, análisis de las fuentes y respuesta frente a las actividades híbridas, y deben apoyar el refuerzo de la resiliencia a largo plazo de sus Estados miembros y de las instituciones, órganos y organismos de la UE frente a amenazas híbridas, haciendo pleno uso de los instrumentos existentes a tal fin. El Consejo recalca la necesidad de actualizar el protocolo de actuación conjunta de la UE para contrarrestar las amenazas híbridas a partir de las enseñanzas identificadas y extraídas en el transcurso de ejercicios anteriores.

7. El Consejo subraya que sigue resultando necesario cooperar con organismos internacionales como las Naciones Unidas, la OSCE y el Consejo de Europa, así como con formatos como el G-7, para defender el orden mundial basado en normas, también en el contexto de la lucha contra las amenazas híbridas, mediante, por ejemplo, el refuerzo de la confianza y otras medidas pertinentes.

8. El Consejo hace hincapié en el compromiso de la UE de mantener la estrecha cooperación de refuerzo mutuo y el apoyo a todos los países socios pertinentes, en particular los países vecinos de la UE, en materia de refuerzo de la resiliencia y lucha contra las amenazas híbridas.

9. El Consejo insta a que se prosigan los esfuerzos de manera continua e ininterrumpida para seguir avanzando en la ejecución de todas las actuaciones relacionadas con la lucha contra las amenazas híbridas al amparo del conjunto común de propuestas para la aplicación de las declaraciones conjuntas sobre la cooperación UE-OTAN, incluso en los ámbitos de la conciencia situacional, la comunicación estratégica, la prevención de crisis y la respuesta ante ellas y el refuerzo de la resiliencia. En este contexto, reitera la necesidad de seguir reforzando el diálogo político en relación con la lucha contra las amenazas híbridas y de realizar ejercicios paralelos y coordinados, con la participación de todos los Estados miembros de la UE y los aliados de la OTAN, e insta a que se complete el nuevo plan de ejercicios paralelos y coordinados de manera oportuna. El Consejo recalca la necesidad de tener en cuenta las enseñanzas identificadas y la importancia de un intercambio de información sin impedimentos, de forma integradora y no discriminatoria.

Asimismo, el Consejo destaca las valiosas contribuciones del Centro de Excelencia para la Lucha contra las Amenazas Híbridas de Helsinki y anima a que coopere con centros de excelencia de la OTAN pertinentes. También acoge con satisfacción los intercambios periódicos y estructurados entre miembros del personal, como por ejemplo la cooperación entre la Célula de Fusión contra las Amenazas Híbridas del Centro de Inteligencia y de Situación de la Unión Europea (INTCEN) y la sección de análisis híbrido de la OTAN.

10. El Consejo reconoce los esfuerzos de los Estados miembros, en cooperación con la Comisión y el Servicio Europeo de Acción Exterior (SEAE), para la realización del estudio sobre los riesgos híbridos contemplado en la medida n.º 1 de la Comunicación conjunta sobre la lucha contra las amenazas híbridas (2016), e insta a proseguir la labor y una posible revisión del estudio sobre los riesgos híbridos para mejorar la respuesta frente a las vulnerabilidades.

Trabajar de manera coherente para aumentar la resiliencia y luchar contra las amenazas híbridas

11. Al desarrollar y emplear tecnologías nuevas y emergentes, como por ejemplo la inteligencia artificial y las técnicas de recopilación de datos, se deben tener debidamente en cuenta las nuevas oportunidades para el aumento de la resiliencia, así como las posibles vulnerabilidades y los efectos en cascada en el contexto de la lucha contra las amenazas híbridas, para reducir los riesgos globales, también durante el proceso de planificación estratégica del Programa Marco de Investigación e Innovación.

12. El Consejo toma nota de que las actividades cibernéticas malintencionadas pueden formar parte de las amenazas híbridas, y en este contexto subraya la pertinencia del conjunto de instrumentos de ciberdiplomacia de la UE.

13. La relación entre las amenazas híbridas y la seguridad económica es un elemento pertinente que se debe tener en cuenta y cuya responsabilidad sigue recayendo principalmente sobre los Estados miembros.

14. Los nuevos instrumentos como el mecanismo con arreglo al Reglamento para el control de las inversiones extranjeras en la Unión se deben emplear de manera eficaz para aumentar la resiliencia y luchar contra las amenazas híbridas, proporcionando medios para identificar y hacer frente a inversiones extranjeras directas que puedan afectar a la seguridad o al orden público.

15. El Consejo invita a la Comisión a que incluya la resiliencia frente a las amenazas híbridas en el proceso de evaluación de impacto para futuras propuestas legislativas pertinentes, entre las que se encuentran futuros programas marco de investigación e innovación.

16. El Consejo subraya la importancia de realizar periódicamente ejercicios y debates basados en situaciones hipotéticas sobre la lucha contra las amenazas híbridas a escala ministerial y a otras escalas. Asimismo, se deben integrar los elementos híbridos en otras actividades de formación y ejercicios de la UE a distintas escalas, con el apoyo de sus Estados miembros y de los órganos pertinentes, concretamente del Centro de Excelencia para la Lucha contra las Amenazas Híbridas, según proceda.

17. Para garantizar la coherencia de las siguientes etapas de la cooperación de la UE para el aumento de la resiliencia y la lucha contra las amenazas híbridas, el Consejo invita a la Comisión y a la Alta Representante a desarrollar un catálogo que enumere de manera exhaustiva las medidas emprendidas hasta la fecha y los documentos pertinentes que se hayan adoptado, con vistas a posibles nuevas iniciativas.

El nexo entre seguridad interior y exterior

18. Las autoridades policiales, de protección civil y otras autoridades pertinentes deben seguir mejorando su preparación para prevenir y luchar contra las amenazas híbridas. Se debe seguir reforzando e integrando la cooperación entre las autoridades nacionales pertinentes, así como con las instituciones, órganos y organismos de la UE en todo el nexo entre seguridad interior y exterior, en función de sus respectivos mandatos, al tiempo que se refuerzan las sinergias y se evita la duplicación de esfuerzos, por medio de, por ejemplo, los métodos de trabajo horizontales, el intercambio voluntario de información y la formación y los ejercicios de carácter intersectorial. A tal fin, se debe seguir evaluando el apoyo y las contribuciones de los mecanismos y organismos de la UE pertinentes, en el marco de sus respectivos mandatos y en el respeto de las restricciones presupuestarias existentes.

19. Las instituciones y órganos de la UE, en colaboración con los Estados miembros, deben seguir desarrollando el empleo de los mecanismos e instrumentos de la UE pertinentes —entre los que se encuentran el Dispositivo de la UE de Respuesta Política Integrada a las Crisis, el Mecanismo de Protección Civil de la Unión y su Centro Europeo de Coordinación de la Respuesta a Emergencias (CECRE)— en apoyo de las respuestas de los Estados miembros frente a amenazas intersectoriales y transfronterizas.

20. El Consejo reconoce la posibilidad de que los Estados miembros invoquen la cláusula de solidaridad (artículo 222 del TFUE) para hacer frente a una grave crisis resultante de una actividad híbrida.

Conciencia situacional y análisis de inteligencia

21. La cooperación de la UE en la mejora de la resiliencia y la lucha contra las amenazas híbridas debe guiarse por una evaluación de las amenazas actualizada periódicamente y una conciencia situacional global. Estos deben ser desarrollados por el INTCEN de la UE y su Célula de Fusión contra las Amenazas Híbridas para mejorar la capacidad de la UE y de sus Estados miembros para detectar, prevenir, perturbar y responder a las actividades híbridas, respetando al mismo tiempo la competencia de los Estados miembros. El Consejo considera que el trabajo de la Célula de Fusión de la UE contra las Amenazas Híbridas debe seguir ampliándose, teniendo en cuenta un nivel adecuado de recursos, incluida la experiencia profesional.

22. El Consejo recuerda sus Conclusiones sobre la lucha contra las amenazas híbridas, de 19 de abril de 2016, en las que se reclamaba la movilización de los instrumentos de la UE para impedir y neutralizar las amenazas híbridas para la Unión y sus Estados miembros, así como para sus socios. El Consejo subraya la necesidad de que se sigan desarrollando las funciones de los Estados miembros y de la UE en materia de conciencia situacional, teniendo en cuenta las fuentes de las amenazas, y de que se haga un mejor uso del análisis de inteligencia del INTCEN de la UE y de su Célula de Fusión, en particular en los procesos de elaboración de políticas y de gestión de crisis de la UE para hacer frente a las amenazas híbridas.

23. El Consejo reconoce la contribución pertinente que las misiones y operaciones de la PCSD podrían aportar, cuando y como proceda, a la hora de identificar y analizar indicadores de posibles acciones híbridas de terceros, incluida la desinformación destinada a desacreditar y obstaculizar la acción de la UE y de sus Estados miembros, y reconoce el valor de seguir explorando la posibilidad de desarrollar esta contribución.

Protección de infraestructuras críticas

24. La protección de las infraestructuras críticas nacionales y europeas, así como de las funciones y servicios esenciales para el buen funcionamiento del Estado, de la economía y de la sociedad, constituye una prioridad clave, incluso en el contexto de la mejora de la resiliencia ante las amenazas híbridas, lo que requiere un planteamiento en el que se involucren todo el gobierno y toda la sociedad. Esta labor debe tener en cuenta las fuertes interdependencias entre las diferentes funciones y servicios críticos, incluidos los servicios financieros, el papel determinante del sector privado, la evolución del entorno de seguridad y los riesgos emergentes, tanto en el ámbito físico como en el cibernético.

25. Por otra parte, además de los requisitos legales, reglamentarios y de supervisión nacionales y de la UE que rigen la resiliencia operativa y la continuidad de las actividades, deben promoverse acuerdos con los propietarios y operadores del sector privado de infraestructuras y servicios para garantizar la continuidad de los servicios críticos y el acceso a los mismos, también más allá de los casos de fuerza mayor, garantizando un nivel aceptable de preparación para responder a todas las amenazas pertinentes, así como la flexibilidad necesaria para hacer frente a los fenómenos de baja probabilidad y grave impacto, mitigarlos y recuperarse de ellos.

26. El Consejo hace hincapié en que, si bien la responsabilidad de la protección de las infraestructuras críticas es fundamentalmente una cuestión de competencia nacional, el alto grado de interdependencia transfronteriza e intersectorial requiere esfuerzos coordinados o, cuando sea necesario, armonizados a escala de la UE, incluso con vistas al funcionamiento ininterrumpido del mercado interior.

27. Tras la evaluación de julio de 2019 sobre la aplicación de la Directiva (2008/114/CE) para la identificación y designación de infraestructuras críticas europeas, el Consejo invita a la Comisión a que consulte a los Estados miembros sobre una posible propuesta de revisión de la Directiva al comienzo del nuevo ciclo legislativo, en particular sobre posibles medidas adicionales para mejorar la protección y la resiliencia de las infraestructuras críticas en la UE, teniendo en cuenta las estrechas interdependencias entre las funciones y los servicios críticos.

28. El Consejo invita a la Comisión a que siga colaborando con los Estados miembros y, cuando proceda, a que desarrolle acuerdos de cooperación no vinculantes entre los Estados miembros que compartan infraestructuras críticas conectadas.

29. El Consejo reconoce la importancia de la Directiva sobre la seguridad de las redes y sistemas de información (Directiva SRI) para el desarrollo de una cultura de gestión de riesgos y seguridad por parte de los operadores en sectores críticos, así como de las capacidades y estrategias nacionales que garanticen un alto nivel de seguridad de las redes y los sistemas de información en su territorio, también en el contexto de las amenazas híbridas. El Consejo invita a los Estados miembros, a la Comisión y a la Agencia de la Unión Europea para la Ciberseguridad (ENISA) a que sigan desarrollando su cooperación sobre la base de la Recomendación de la Comisión sobre la respuesta coordinada a los incidentes y crisis de ciberseguridad a gran escala (plan director) a todos los niveles pertinentes.

Contrarrestar la desinformación y garantizar unas elecciones libres y justas

30. El Consejo acoge con satisfacción el informe sobre la aplicación del Plan de Acción contra la Desinformación y reconoce que la aplicación continuada del Plan de Acción sigue ocupando un lugar central en los esfuerzos de la UE. El Consejo subraya la necesidad de que se revise periódicamente y, en caso necesario, se actualice el Plan de Acción para garantizar un enfoque eficaz a largo plazo.

31. El Consejo señala que el trabajo de la División de Comunicaciones Estratégicas del SEAE y, en particular, de los tres grupos de trabajo (Este, Balcanes Occidentales y Sur) debe contar con el apoyo de recursos suficientes que permitan la planificación, ejecución y evaluación a largo plazo. Entre sus tareas, los tres grupos de trabajo deberían ser capaces de detectar, analizar y hacer frente de manera continua las actividades de desinformación de los agentes estatales extranjeros y de los agentes externos no estatales. Los grupos de trabajo deberían seguir contribuyendo a una comunicación positiva efectiva y basada en hechos y a la promoción de los principios, valores y políticas de la Unión en los países vecinos orientales y meridionales de la UE y en los Balcanes Occidentales, así como al fortalecimiento del entorno general de los medios de comunicación y de la sociedad civil en sus regiones correspondientes. El Consejo invita al SEAE a que evalúe las necesidades y las posibilidades de reforzar su labor de comunicación estratégica en otras zonas geográficas, como el África subsahariana, manteniendo al mismo tiempo la capacidad necesaria para llevar a cabo las actuales tareas de comunicación estratégica.

32. El Consejo reconoce que es necesario un enfoque global a todos los niveles para hacer frente a los desafíos de la desinformación, incluidas las injerencias destinadas a socavar unas elecciones europeas libres y justas, haciendo el mejor uso posible de todos los instrumentos disponibles en línea y fuera de línea. Ello debe incluir el control y el análisis de la desinformación y de la injerencia manipuladora, el cumplimiento de las normas europeas de protección de datos, la aplicación de las salvaguardias electorales, los esfuerzos para mejorar el pluralismo de los medios de comunicación, el periodismo profesional y la alfabetización mediática, así como la sensibilización de los ciudadanos. El Consejo recomienda que se siga consolidando una red transeuropea activa e independiente de verificadores de hechos e investigadores contra la desinformación. El Consejo reconoce la importancia y el papel de la sociedad civil, del mundo académico y del sector privado en la lucha contra la desinformación y el desarrollo de la resiliencia.

33. El Consejo reconoce el potencial del sistema de alerta rápida en la lucha contra la desinformación, en particular en lo que se refiere a la injerencia en las elecciones. Insta a la Comisión y al SEAE a que, junto con los Estados miembros, sigan desarrollando el sistema de alerta rápida hacia una plataforma global para que los Estados miembros y las instituciones de la UE refuercen la cooperación, la coordinación y el intercambio de información, como la investigación y los conocimientos analíticos, las mejores prácticas y los productos de comunicación, a fin de apoyar que se aborden las campañas de desinformación como parte de una serie de esfuerzos europeos y nacionales.

34. El Consejo reconoce la utilidad de las medidas y recomendaciones presentadas por la Comisión el 12 de septiembre de 2018 en su conjunto de medidas relativas a las elecciones para garantizar la seguridad de los comicios europeos. El Consejo alienta a la Comisión y a los Estados miembros a que estudien las posibilidades de proseguir las actividades de las redes europeas de cooperación en materia electoral para apoyar el intercambio de información y mejores prácticas. El Consejo celebra los esfuerzos de la Comisión por implicar a todas las partes interesadas pertinentes y apoyar una amplia gama de medidas, como el ejercicio sobre la ciberseguridad de las elecciones europeas (EU ELEx19), teniendo en cuenta las competencias nacionales en este ámbito.

35. El Consejo reconoce la necesidad de que se siga trabajando con las plataformas de medios sociales para lograr niveles más elevados de responsabilidad, transparencia y rendición de cuentas en la lucha contra la desinformación. Además, debe concederse un acceso sin trabas a los datos anónimos de los proveedores de plataformas de medios sociales para la investigación académica, a fin de facilitar la adopción de políticas basadas en pruebas. El Consejo solicita a la Comisión que presente iniciativas sobre la forma de abordar la desinformación en las plataformas en línea. Estas iniciativas deben basarse en una evaluación de la aplicación del Código de Buenas Prácticas en materia de Desinformación, que debe tener en cuenta el trabajo analítico y los informes realizados por el mundo académico y las organizaciones de la sociedad civil, el informe de seguimiento del Código elaborado por el Grupo de Entidades Reguladoras Europeas para los Servicios de Comunicación Audiovisual, así como las enseñanzas extraídas de las elecciones al Parlamento Europeo de mayo de 2019. En este contexto, el Consejo invita a la Comisión a que estudie la manera, incluidos los posibles mecanismos de aplicación para las plataformas en línea, de seguir mejorando la aplicación del Código de Buenas Prácticas, en particular mediante la inclusión de una evaluación independiente del cumplimiento de los compromisos por parte de los signatarios.

Seguridad de las instituciones, órganos y organismos de la UE

36. La seguridad del personal, las instituciones, los órganos y los organismos de la UE contra amenazas híbridas y otras actividades malintencionadas es un interés compartido por la UE y sus Estados miembros. El Consejo insta a las instituciones, órganos y organismos de la UE, con el apoyo de los Estados miembros, a que garanticen la capacidad de la Unión para proteger su integridad y mejorar la seguridad de las redes de información y comunicación y de los procesos de toma de decisiones de la UE frente a actividades malintencionadas de todo tipo, sobre la base de una evaluación exhaustiva de las amenazas. A tal fin, as instituciones, los órganos y los organismos, con el apoyo de los Estados miembros, deben desarrollar y aplicar un conjunto completo de medidas para garantizar su seguridad, de conformidad con el mandato del Consejo Europeo de junio de 2019. El Consejo destaca la importancia de que se garantice la interoperabilidad de la infraestructura informática de la UE para el intercambio de información clasificada entre las instituciones, órganos y organismos y Estados miembros de la UE.