Consejo de la Unión Europea

Bruselas, 19 de noviembre de 2018
(OR. en)

14413/18

CYBER 285
CSDP/PSDC 669
COPS 444
POLMIL 214
EUMC 193
RELEX 978
JAI 1154
TELECOM 415
CSC 328
CIS 13
COSI 290

RESULTADO DE LOS TRABAJOS

De:	Secretaría General del Consejo
Fecha:	19 de noviembre de 2018
A:	Delegaciones
Asunto:	Marco político de ciberdefensa de la UE (actualización de 2018)

En el anexo se remite, a la atención de las delegaciones, el marco político de ciberdefensa de la UE (actualización de 2018), adoptado por el Consejo en su sesión n.° 3652 celebrada el 19 de noviembre de 2018.

ANEXO

MARCO POLÍTICO DE CIBERDEFENSA DE LA UE

(según actualización de 2018)

Ámbito de aplicación y objetivos

Para responder a los retos cambiantes en el ámbito de la seguridad, la UE y sus Estados miembros deben reforzar la ciberresiliencia y desarrollar capacidades sólidas en ciberseguridad y defensa.

El marco político de ciberdefensa de la UE apoya el desarrollo de las capacidades en ciberdefensa de los Estados miembros de la UE y el refuerzo de la ciberprotección de la infraestructura de seguridad y defensa de la UE, sin perjuicio de la legislación nacional de los Estados miembros y de la UE, incluido el ámbito de aplicación de la ciberdefensa, si está definido.

El ciberespacio es el quinto ámbito de actuación, junto con los ámbitos de tierra, mar, aire y espacio. La ejecución exitosa de las misiones y operaciones de la UE depende cada vez más del acceso ininterrumpido a un ciberespacio seguro y ello requiere unas capacidades operativas sólidas y resilientes en el ámbito cibernético.

El objetivo de actualizar el marco político es seguir desarrollando la política de ciberdefensa de la UE teniendo en cuenta avances importantes que se han producido en foros y ámbitos de actuación pertinentes y la aplicación del marco desde 2014. El marco define unos ámbitos prioritarios de actuación para la ciberdefensa y aclara el cometido de los diversos agentes europeos en la materia, al tiempo que respeta plenamente las responsabilidades y competencias de los agentes de la UE y de los Estados miembros, así como el marco institucional de la UE y la autonomía de su proceso decisorio.

Contexto

En las Conclusiones del Consejo Europeo sobre la PCSD de diciembre de 2013 y en las Conclusiones del Consejo sobre la PCSD de noviembre de 2013 se pedía la elaboración de un marco político de la UE para la ciberdefensa, a partir de una propuesta de la Alta Representante, en cooperación con la Comisión Europea y con la Agencia Europea de Defensa (AED). El Consejo adoptó el marco político de ciberdefensa de la UE el 14 de noviembre de 2014[1] y, desde entonces, a través de su aplicación, los resultados concretos han contribuido a mejorar significativamente las capacidades en ciberdefensa de los Estados miembros. Como parte del Informe anual sobre la aplicación del Marco político de ciberdefensa[2], y teniendo en consideración las iniciativas de la UE en el ámbito de la seguridad y la defensa, especialmente la revisión anual coordinada de la defensa, la cooperación estructurada permanente, el Fondo Europeo de Defensa, el pacto sobre la vertiente civil de la política común de seguridad y defensa y la revisión de 2018 del Plan de Desarrollo de Capacidades y el Plan de Desarrollo de Capacidades Civiles, los Estados miembros pidieron una actualización del Marco político de ciberdefensa de la UE.

La ciberseguridad es una prioridad de la Estrategia Global sobre Política Exterior y de Seguridad de la Unión Europea y del nivel de ambición de la UE[3]. La Estrategia Global insiste en la necesidad de aumentar las capacidades para proteger a la UE y a sus ciudadanos y para responder a las crisis externas. La Estrategia Global subraya la necesidad de reforzar la UE como una comunidad de la seguridad. En este contexto, los esfuerzos en seguridad y defensa también potenciarán el papel estratégico de la UE y su capacidad para actuar de manera autónoma, siempre y cuando sea necesario, y en colaboración con sus socios, en la medida de lo posible. Estos objetivos requieren más cooperación en el desarrollo de capacidades, promoviendo la eficacia y la interoperabilidad de las capacidades civiles y militares resultantes.

---

1 Documento del Consejo n.º 15585/14 de 18.11.2014.
2 Documento del Consejo n.º 15870/17 de 19.12.2017.
3 Conclusiones del Consejo sobre la aplicación de la Estrategia Global de la UE en materia de Seguridad y Defensa, 14.11.2016

El paquete común de propuestas para la aplicación de la declaración conjunta firmada por el presidente del Consejo Europeo, el presidente de la Comisión Europea y el secretario general de la Organización del Tratado del Atlántico Norte el 8 de julio de 2016[4] incluye acciones concretas para ampliar la cooperación de la UE y la OTAN en ciberseguridad y defensa, en particular en el contexto de las misiones y las operaciones, así como en relación con el desarrollo de capacidades en ciberdefensa, la investigación y la tecnología, la formación, la educación, los ejercicios y la integración de la perspectiva cibernética en la gestión de las crisis. Esta cooperación se desarrolla en el pleno respeto de los principios de apertura, transparencia, inclusión, reciprocidad y autonomía decisoria de la UE. Un acuerdo técnico firmado en febrero de 2016 entre el Equipo de respuesta a emergencias informáticas de las instituciones, órganos y organismos de la Unión Europea (CERT-UE) y la Capacidad de respuesta ante incidentes informáticos de la OTAN está facilitando el intercambio de información técnica en ambas organizaciones para mejorar la prevención, la detección y la respuesta ante ciberincidentes.

Hay que recordar que varias políticas de la UE contribuyen a los objetivos de la política de ciberdefensa que figuran en el presente documento; este marco tiene en cuenta asimismo el apoyo pertinente en materia de reglamentación, política y tecnología en el ámbito civil. Por ejemplo, en julio de 2016, el Parlamento Europeo y el Consejo adoptaron la Directiva sobre ciberseguridad de las redes y sistemas de información[5] (SRI), que mejorará la preparación general de los Estados miembros frente a las ciberamenazas y fomentará la cooperación a escala de la UE. Dicha Directiva establece medidas con el objeto de lograr un elevado nivel común de seguridad de las redes y sistemas de información dentro de la Unión a fin de mejorar el funcionamiento del mercado interior. La fecha límite para la transposición de la Directiva es el 9 de mayo de 2018.

---

4 Conclusiones del Consejo sobre la ejecución de la declaración conjunta del presidente del Consejo Europeo, el presidente de la Comisión Europea y el secretario general de la Organización del Tratado del Atlántico Norte (6 de diciembre de 2016, doc. 15283/16; 5 de diciembre de 2017, doc. 14802/17)

5 Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, DO L 194 de 19.7.2016, p. 1.

La propuesta, de septiembre de 2017, de un nuevo Reglamento de Ciberseguridad de la UE incluye el nuevo mandato de la Agencia de la Unión Europea para la Ciberseguridad (ENISA) y la creación de un marco de certificación para toda la UE. Una vez en vigor, el marco de certificación debe favorecer unas normas estrictas para los servicios, productos y procesos de las TIC, al tiempo que debe ser fuente de ventaja competitiva y aumentar la confianza de los consumidores y compradores. Asimismo, en septiembre de 2017, la Comisión dio un paso más para preparar a la UE ante el caso de que se produjeran incidentes de ciberseguridad transfronterizos de gran envergadura («Blue Print») y ahora está trabajando con los Estados miembros y otras instituciones, agencias y organismos en el desarrollo de la cooperación europea en caso de crisis de ciberseguridad, estableciendo la aplicación práctica y la documentación relativa a todas las partes, procesos y procedimientos pertinentes dentro del contexto de los mecanismos actuales de gestión de crisis y catástrofes de la UE, en particular el Dispositivo Integrado de Respuesta Política a las Crisis.

Las Conclusiones del Consejo sobre reforzar el sistema de ciberresiliencia de Europa, de noviembre de 2016, señalaban el objetivo común de contribuir a la autonomía estratégica de Europa, tal como se ponía de manifiesto en las Conclusiones del Consejo de noviembre de 2016 relativas a la Estrategia Global sobre Política Exterior y de Seguridad, también en el ámbito del ciberespacio. El Consejo Europeo reafirmó este mensaje en junio de 2018 y también destacó la necesidad de reforzar las capacidades de lucha contra las amenazas en materia de ciberseguridad procedentes de fuera de la UE.

En 2017, el Consejo adoptó un marco para una respuesta diplomática conjunta de la UE a las actividades informáticas malintencionadas («el conjunto de instrumentos de ciberdiplomacia»)[6]. Se espera que el marco fomente la cooperación, ayude a reducir las amenazas e influya en el comportamiento de los agresores potenciales a largo plazo. El marco hace uso de las medidas de PESC, en particular de las medidas restrictivas, para impedir las actividades cibernéticas malintencionadas y responder a ellas. Los autores de actividades cibernéticas malintencionadas deben responder de sus acciones y se anima a los Estados miembros a seguir desarrollando su capacidad para responder a dichas actividades malintencionadas, de forma coordinada en línea con el conjunto de instrumentos de ciberdiplomacia. Los Estados no deberían llevar a cabo ni apoyar deliberadamente actividades de las tecnologías de la información y la comunicación contrarias a sus obligaciones en virtud del Derecho internacional, ni tampoco permitir deliberadamente que se utilice su territorio para cometer hechos internacionalmente ilícitos utilizando las tecnologías de la información y la comunicación.

La Comisión y la Alta Representante presentaron en septiembre de 2017 una comunicación conjunta[7] sobre ciberseguridad para mitigar los riesgos derivados de las nuevas amenazas. Dicha comunicación incluye la ciberdefensa como uno de los principales ámbitos de actuación, y el presente marco es uno de los pilares de su aplicación concreta[8].

En sus Conclusiones sobre ciberseguridad de noviembre de 2017, el Consejo reconocía la vinculación cada vez mayor entre ciberseguridad y defensa, e instaba a incrementar la cooperación en materia de defensa cibernética, en particular fomentando la cooperación entre las comunidades civil y militar de respuesta a incidentes. También destacaba que un incidente o ataque cibernético particularmente grave podría constituir motivo suficiente para que un Estado miembro invoque las cláusulas de solidaridad o de asistencia mutua de la UE.

---

6 Conclusiones del Consejo sobre un marco para una respuesta diplomática conjunta de la UE a las actividades informáticas malintencionadas («conjunto de instrumentos de ciberdiplomacia»), doc. 9916/17 de 7 de junio de 2017

7 Comunicación conjunta al Parlamento Europeo y al Consejo: «Resiliencia, disuasión y defensa: fortalecer la ciberseguridad de la UE» (13 de septiembre de 2017, JOIN (2017) 450 final).

8 Conclusiones del Consejo sobre la Comunicación conjunta al Parlamento Europeo y al Consejo titulada «Resiliencia, disuasión y defensa: fortalecer la ciberseguridad de la UE» (20 de noviembre de 2017, 14435/17)

El 11 de diciembre de 2017 se puso en marcha la cooperación estructurada permanente (CEP). Se ha establecido este marco de cooperación ambicioso, vinculante e inclusivo entre 25 Estados miembros, que incluye un compromiso para aumentar los esfuerzos en cooperación en materia de ciberdefensa, así como en los proyectos de CEP correspondientes. El primer conjunto de proyectos de CEP definido en 2017 por los Estados miembros participantes en la CEP incluye dos proyectos relacionados con la ciberdefensa: «Equipos de respuesta telemática rápida y de asistencia mutua en el ámbito de la ciberseguridad» y «Plataforma de intercambio de información sobre respuestas a ciberamenazas e incidentes de ciberseguridad». Se prevén nuevos conjuntos de proyectos de CEP. La CEP desarrollará las capacidades en ciberdefensa y reforzará, por tanto, la cooperación entre los Estados miembros participantes y aumentará la interoperabilidad.

El Plan de Desarrollo de Capacidades actualizado refrendado por la Junta Directiva de la Agencia Europea de Defensa en junio de 2018 define la ciberdefensa como un elemento clave, reconociendo la necesidad de realizar operaciones defensivas en el ámbito cibernético en cualquier contexto operativo, sobre la base de un conocimiento sofisticado, actual y predictivo de la situación del ciberespacio, en particular la capacidad de combinar grandes cantidades de datos y de inteligencia procedentes de numerosas fuentes para dar apoyo a una toma de decisiones rápida, así como sobre la base de una mayor automatización de la recopilación de datos, análisis y procesos de apoyo a la toma de decisiones. El Plan de Desarrollo de Capacidades de 2018 define las prioridades de capacidades de ciberdefensa en las siguientes áreas: cooperación y sinergias con los agentes pertinentes en los ámbitos de ciberdefensa y ciberseguridad; actividades de investigación y tecnología en ciberdefensa; marcos de ingeniería de sistemas para las ciberoperaciones; educación, formación, ejercicios y evaluación; abordar los retos en ciberdefensa en los ámbitos de tierra, mar, aire y espacio.

Finalmente, en los últimos años, ha quedado clara la necesidad de que la comunidad internacional evite los conflictos, coopere y estabilice el ciberespacio. La UE promueve, en estrecha colaboración con otras organizaciones internacionales, en particular las Naciones Unidas, la OSCE y el Foro Regional de la ASEAN, un marco estratégico para la prevención de conflictos, la cooperación y la estabilidad en el ciberespacio, que incluye (i) la aplicación del Derecho internacional, y en particular la Carta de las Naciones Unidas en su totalidad, en el ámbito del ciberespacio; (ii) el respeto de normas, reglas y principios universales y no vinculantes de comportamiento responsable de los Estados; (iii) el desarrollo y la aplicación de medidas regionales de fomento de la confianza. El marco político de ciberdefensa también debería apoyar esta tarea.

Prioridades

Se han determinado seis ámbitos prioritarios en el marco actualizado. Un objetivo central del presente Marco político es el desarrollo de las capacidades en ciberdefensa y la protección de las redes de comunicación e información de la PCSD de la UE. Otros ámbitos prioritarios son: formación y ejercicios, investigación y tecnología, cooperación civil-militar y cooperación internacional. En el ámbito de la formación, se ha hecho hincapié en la mejora de la formación en ciberdefensa en los Estados miembros y de la formación en concienciación en materia cibernética de la cadena de mando de la PCSD. También es importante que la dimensión cibernética se aborde adecuadamente mediante ejercicios que permitan mejorar la capacidad de la UE para responder a crisis cibernéticas e híbridas mejorando los procedimientos de toma de decisiones y la disponibilidad de la información. El ciberespacio es un ámbito que avanza muy rápidamente y es necesario apoyar nuevos desarrollos tecnológicos, tanto en el ámbito civil como en el militar. La cooperación civil-militar en el ámbito cibernético es clave para garantizar una respuesta coherente ante las ciberamenazas. Por último en orden, pero no en importancia, fomentar la cooperación con los socios internacionales podría contribuir a mejorar la ciberseguridad tanto dentro como fuera de la UE y promover los principios y valores de la UE.

El presente marco plantea propuestas y oportunidades de coordinación entre las instituciones, los organismos y las agencias pertinentes de la UE. También refleja el importante papel del sector privado en el desarrollo de la tecnología en el ámbito de la ciberseguridad y la ciberdefensa.

Además, el marco apoya la integración de la ciberdefensa en los mecanismos de gestión de crisis de la Unión cuando, para hacer frente a las consecuencias de una cibercrisis, puedan ser de aplicación las disposiciones correspondientes del Tratado de la UE y del Tratado de Funcionamiento de la UE[9].

1. Apoyar el desarrollo de las capacidades de ciberdefensa de los Estados miembros

La mejora de las capacidades y tecnologías en materia de ciberdefensa deberá abordar todos los aspectos del desarrollo de capacidades, es decir, doctrina, liderazgo, organización, personal, formación, industria, tecnología, infraestructuras, logística e interoperabilidad. Para ello, los Estados miembros deberán aumentar sus esfuerzos para garantizar la eficacia de las capacidades en ciberdefensa. El SEAE, la Comisión y la AED deberán trabajar conjuntamente y apoyar dichos esfuerzos.

Es necesaria una evaluación permanente de las vulnerabilidades de las infraestructuras de información que sirven de apoyo a las misiones y operaciones PCSD, además de una comprensión en tiempo cuasirreal de la eficacia de la protección. Desde un punto de vista operativo, uno de los principales ámbitos de atención de las actividades de ciberdefensa será mantener la disponibilidad, la integridad y la confidencialidad de las redes de comunicación e información de la PCSD, a no ser que el mandato de las correspondientes operaciones o misiones especifique algo distinto. Además, el SEAE, en cooperación con los Estados miembros, seguirá integrando las capacidades cibernéticas en las misiones y operaciones de la PCSD.

Los autores de las actividades cibernéticas malintencionadas deberán responder de sus actos. Es importante que los Estados miembros de la UE, apoyados por el SEAE, fomenten la cooperación mutua para responder a las actividades cibernéticas malintencionadas. Se ha elaborado el conjunto de instrumentos de ciberdiplomacia con el fin de contribuir a lograr esa respuesta mutua. El SEAE y la AED organizarán regularmente ejercicios basados en el conjunto de instrumentos de ciberdiplomacia en los que los Estados miembros de la UE podrán poner esto en práctica.

---

[9] Artículos 222 del TFUE y 42, apartado 7, del TUE, teniendo en cuenta debidamente el art. 17 del TUE.

Teniendo en cuenta que tanto en la legislación nacional de los Estados miembros como en la legislación de la UE la definición de ciberdefensa, cuando existe, es muy amplia y diversificada, es necesario desarrollar un concepto común y general sobre el ámbito de la ciberdefensa.

Como las operaciones militares PCSD se apoyan en una infraestructura de mando, control, comunicaciones y ordenadores (C4) facilitada por los Estados miembros, al planificar los requisitos en materia de ciberdefensa para infraestructuras de información se requiere cierto grado de convergencia estratégica.

Aprovechando la labor del Equipo de proyecto de ciberdefensa de la AED orientado al desarrollo de capacidades de ciberdefensa, la AED y los Estados miembros:

- utilizarán el Plan de Desarrollo de Capacidades y otros instrumentos, como la revisión anual coordinada de la defensa, que permitan facilitar y apoyar la cooperación entre Estados miembros con el fin de mejorar el grado de convergencia de los Estados miembros en la planificación de los requisitos en materia de ciberdefensa desde un punto de vista estratégico, en particular con respecto a la supervisión, conocimiento de la situación, prevención, detección y protección, intercambio de información, capacidades de informática forense y de análisis de programas malintencionados, lecciones extraídas, contención de daños, capacidades de recuperación dinámicas, almacenamiento de datos distribuidos y copias de seguridad de los datos;
- apoyarán los proyectos de puesta en común y uso compartido en materia de ciberdefensa vigentes y futuros para operaciones militares (por ejemplo, informática forense, mejora de la interoperabilidad, elaboración de normas);
- elaborarán un conjunto uniforme de objetivos y requisitos que determinen el grado mínimo de ciberseguridad y confianza que deberán alcanzar los Estados miembros, aprovechando la experiencia ya adquirida a escala de la UE;

El SEAE y la AED:

- facilitarán los intercambios entre Estados miembros en materia de doctrinas nacionales sobre ciberdefensa, así como de programas de contratación, retención y reservistas, orientados a la ciberdefensa.

La AED:

- estudiará el alcance de los requisitos en materia de ciberdefensa militar en la legislación nacional y en las mejores prácticas de los Estados miembros. El principal objetivo del estudio será desarrollar una arquitectura de empresa para la ciberdefensa a fin de incluir el alcance, las funciones y los requisitos al respecto que utilizan los Estados miembros con arreglo a la legislación nacional y de la UE.

Los Estados miembros, con carácter voluntario:

- mejorarán la cooperación entre sus equipos de respuesta a emergencias informáticas (CERT) militares con el fin de mejorar a su vez la prevención y tratamiento de incidentes;
- aprovecharán la cooperación estructurada permanente (CEP) para aumentar la cooperación en materia de ciberdefensa, en particular para desarrollar nuevos proyectos
- aprovecharán el Fondo Europeo de Defensa para desarrollar capacidades de ciberdefensa conjuntamente;
- desarrollarán un concepto común de la aplicación de la cláusula de asistencia mutua en el ámbito de la ciberseguridad, preservando al mismo tiempo su flexibilidad;
- desarrollarán unos requisitos de referencia en materia de ciberdefensa para las infraestructuras de información;
- en la medida en que la mejora de las capacidades de ciberdefensa dependa de conocimientos especializados de carácter civil en materia de seguridad de las redes y de la información, aprovecharán los conocimientos y la experiencia de la ENISA, de las autoridades de los Estados miembros en el Grupo de cooperación SRI y de otras posibles entidades a escala de la UE con experiencia en ciberseguridad civil.

Los Estados miembros, el SEAE/el Estado Mayor de la UE, la EESD y la AED:

- considerarán la posibilidad de impulsar la formación en materia de ciberdefensa, con vistas a la certificación para los grupos de combate de la UE.

La Comisión, en cooperación con los Estados miembros:

- tendrá en cuenta la ciberdefensa en los planes de trabajo del Programa Europeo de Desarrollo Industrial en materia de Defensa y del Fondo Europeo de Defensa.

2. Mejorar la protección de las redes de comunicación y los sistemas de información de la PCSD utilizados por entidades de la UE

Sin perjuicio del papel de los equipos de respuesta a emergencias informáticas de las instituciones, órganos y organismos de la Unión Europea (CERT-UE) como estructuras centrales de coordinación de la respuesta de la UE ante incidentes cibernéticos para todas las instituciones, organismos y agencias de la Unión y en el marco de las correspondientes normas relativas al presupuesto de la Unión, el SEAE impulsará una comprensión adecuada y autónoma de los asuntos relativos a la seguridad y a las redes y elaborará su propia capacidad de seguridad de las tecnologías de la información. Su objetivo será mejorar la resiliencia de las redes PCSD del SEAE, centrándose en la prevención, detección, respuesta ante incidentes, conocimiento de la situación, intercambio de información y mecanismos de alerta temprana.

La protección de los sistemas de comunicación e información del SEAE y el desarrollo de capacidades de seguridad en tecnologías de la información son responsabilidades de la Dirección de Presupuesto y Administración (DGBA) del SEAE. El Estado Mayor de la Unión Europea (EMUE), la Dirección de Gestión de Crisis y Planificación (CMPD) y la Capacidad Civil de Planificación y Ejecución (CPCC) proporcionarán recursos y apoyo adicionales. Esta capacidad de la seguridad de las tecnologías de la información abarcará tanto sistemas clasificados como no clasificados y formará parte de las entidades operativas existentes.

También es necesario simplificar las normas de seguridad de los sistemas de información proporcionadas por los diversos agentes institucionales de la UE durante el desempeño de las misiones y operaciones PCSD. En este contexto, podría considerarse la posibilidad de crear una cadena de mando unificada para mejorar la resiliencia de las redes utilizadas en la aplicación de la PCSD.

Para lograr una mejor coordinación y con objeto de reforzar la protección y la resiliencia de las redes y los sistemas de comunicación e información de la PCSD, en 2017 se creó una junta de cibergobernanza del SEAE dependiente del Secretario General del SEAE.

El SEAE/la DGBA:

- reforzarán las capacidades de seguridad de las tecnologías de la información en el seno del SEAE, basándose en la capacidad y los procedimientos técnicos existentes, centrándose en la prevención, la detección, la respuesta ante incidentes, el conocimiento de la situación, el intercambio de información y los mecanismos de alerta temprana. Se mejorará la estrategia de cooperación con el CERT-UE y con las capacidades de seguridad existentes en la UE en materia cibernética.

El SEAE/la DGBA, junto con la MPCC, el EMUE, la CMPD y la CPCC:

- establecerán normas y directrices coherentes para la seguridad de las tecnologías de la información, teniendo también en cuenta los requisitos técnicos de la ciberdefensa en un contexto PCSD para las estructuras, misiones y operaciones, y tomando en consideración los marcos y políticas de cooperación ya existentes en la UE para lograr la convergencia en materia de normas, políticas y organización;

El SEAE/la Capacidad única de análisis de inteligencia (SIAC):

- mejorarán, aprovechando las estructuras ya existentes, sus evaluaciones de la amenaza cibernética y las capacidades de inteligencia necesarias para detectar nuevos riesgos en este ámbito, y presentarán evaluaciones de riesgos periódicas basadas en la evaluación estratégica de amenazas y en la información sobre incidentes en tiempo cuasirreal coordinadas entre las estructuras pertinentes de la UE y facilitadas en diferentes niveles de clasificación.

El SEAE/la SIAC y el CERT-UE:

- promoverán el intercambio de información en tiempo real sobre amenazas cibernéticas entre los Estados miembros y las entidades pertinentes de la UE. A tal efecto, se crearán mecanismos de intercambio de información y medidas de creación de confianza mutua entre las autoridades nacionales y europeas pertinentes mediante un planteamiento voluntario que parta de la cooperación ya existente.

El SEAE/el Estado Mayor y la MPCC:

- impulsarán e integrarán en mayor medida en la planificación estratégica un concepto en materia de ciberdefensa para las operaciones y misiones militares de la PCSD;
- desarrollarán, en cooperación con el cuartel general de las operaciones, un procedimiento operativo normalizado cibernético.

El SEAE/la CPCC y la CMPD:

- seguirán desarrollando e integrando en la planificación estratégica un concepto de ciberdefensa para las misiones civiles de la PCSD;
- reforzarán las capacidades de ciberdefensa de las misiones civiles de la PCSD aprovechando las infraestructuras existentes y promoviendo la normalización y armonización de las tecnologías utilizadas en las misiones y operaciones de la PCSD, aprovechando, cuando proceda, la experiencia del CERT-UE, la ENISA y la AED;
- en el proceso de refuerzo de la vertiente civil de la PCSD, seguirán estudiando el posible apoyo en materia de ciberseguridad a los países de acogida de las misiones civiles de la PCSD.

El SEAE:

- seguirá desarrollando los requisitos comunes para las misiones y operaciones militares y civiles de la PCSD;
- mejorará la coordinación de la ciberdefensa para cumplir los objetivos relacionados con la protección de las redes utilizadas por los agentes institucionales de la UE que sirven de apoyo a la PCSD, aprovechando la experiencia a escala de la UE ya existente;
- revisará periódicamente los requisitos en materia de recursos y otras decisiones pertinentes basadas en un entorno de amenazas cambiante, en consulta con los Estados miembros y otras instituciones de la UE.

3. Fomento de la cooperación cívico-militar

El ciberespacio es un ámbito en rápida evolución, y es necesario reforzar los nuevos avances tecnológicos con sistemas de seguridad, tanto en el ámbito civil como en el militar. En la medida de lo posible, en aquellos casos en que unos avances tecnológicos similares aporten soluciones para las aplicaciones civiles y militares debe preverse una coordinación entre el ámbito civil y el militar. En otros casos, las capacidades militares y los sistemas armamentísticos son tan específicos que no hay posibilidad de compartirlos con tecnologías civiles. Sin perjuicio de la organización interna y de la legislación de los Estados miembros, puede estudiarse la cooperación cívico-militar en el ámbito cibernético, entre otras cosas, para el intercambio de prácticas idóneas, el intercambio de información y de mecanismos de alerta temprana, las evaluaciones de riesgo de las respuestas ante incidentes y las campañas de sensibilización al respecto, y para la formación y los ejercicios.

Mejorar la ciberseguridad civil es un importante factor que contribuye a la resiliencia global de la seguridad de las redes y de la información. La Directiva SRI aumenta el grado de preparación a escala nacional y refuerza la cooperación a escala de la Unión entre los Estados miembros, tanto en un plano estratégico como operativo. Dicha cooperación incluye tanto a las autoridades nacionales que supervisan las políticas de ciberseguridad como a los CERT nacionales y al CERT-UE. Debe reforzarse la cooperación entre las vertientes civil y militar de los CERT teniendo debidamente en cuenta esta evolución. El nuevo Reglamento europeo de ciberseguridad tiene por objeto mejorar la resistencia a los ciberataques y proporcionar un marco de certificación de la ciberseguridad para productos y servicios, aumentando así la confianza en el ámbito digital.

Se anima a la AED, a la Agencia de Seguridad de las Redes y de la Información de la Unión Europea (ENISA), al Centro Europeo de Ciberdelincuencia (EC3) y al CERT-UE, así como a otros organismos e instituciones de la UE, a que, en el marco de sus mandatos respectivos y sin invadir las competencias de los Estados miembros, sigan mejorando su cooperación en los siguientes ámbitos:

- elaboración de perfiles comunes sobre competencias en materia de ciberseguridad y ciberdefensa basados en las mejores prácticas internacionales y de certificación utilizadas por las instituciones, órganos y organismos de la UE, teniendo también en cuenta las normas de certificación del sector privado;
- contribución a un mayor impulso y adaptación de las normas organizativas y técnicas en materia de ciberseguridad y ciberdefensa del sector público para su uso en el sector de la defensa y la seguridad. Cuando proceda, se utilizarán los trabajos en curso de la ENISA y la AED;
- creación o prosecución del desarrollo de mecanismos de trabajo y disposiciones para intercambiar las mejores prácticas en particular sobre la educación, la formación y los ejercicios, así como sobre investigación y tecnología y otros ámbitos que facilitan sinergias entre los planos civil y militar;
- aprovechamiento de las experiencias existentes a escala de la UE en materia de prevención de la ciberdelincuencia, investigación e informática forense y aumento de su utilización en el desarrollo de capacidades de ciberdefensa.

Los Estados miembros, con carácter voluntario:

- reforzarán la cooperación entre los planos civil y militar de los CERT entre los Estados miembros.

El SEAE, la Comisión y los Estados miembros:

- incluirán la ciberdefensa en los procedimientos de la UE de gestión de crisis y catástrofes (a través del proceso de aplicación del plan director).

4. Investigación y tecnología

Los operadores de infraestructuras y servicios de TIC con fines civiles y de defensa se enfrentan a retos similares en materia de ciberseguridad, como resultado de unos requisitos comunes en cuanto a su capacidad tecnológica y operativa. Se da por descontado que unas necesidades comunes en materia de I+T y unos requisitos comunes de los sistemas mejorarán la interoperabilidad de los mismos a largo plazo y reducirán los costes del desarrollo de soluciones. Lograr economías de escala es una necesidad para hacer frente al número creciente de amenazas y puntos débiles. Ello debería facilitar a su vez la preservación y el crecimiento de una industria ciberdefensiva competitiva en Europa.

El desarrollo de la capacidad en ciberdefensa tiene una importante dimensión de I+T. En el marco de la Agenda de Investigación Europea en Ciberdefensa (CDRA), la AED ha proporcionado una sólida base para establecer las futuras prioridades de financiación en I+T en el marco intergubernamental. El plan estratégico de investigación subsiguiente, elaborado en el correspondiente grupo ad hoc de la AED, establece un orden de prioridad informado en el ámbito de las tecnologías relacionadas con la cibernética necesarias para el plano militar, e señala al mismo tiempo las posibilidades de esfuerzo e inversiones en materia de doble uso tanto en contextos nacionales como multinacionales o financiados por la UE.

Es esencial impulsar las capacidades tecnológicas en Europa para mitigar las amenazas y paliar los puntos débiles. La industria seguirá siendo el motor principal de la tecnología y la innovación relacionadas con la ciberdefensa. Algunos de los ámbitos que es necesario abordar son la criptografía, los sistemas empotrados seguros, la detección de programas malintencionados, las técnicas de simulación y visualización, la protección de las redes y sistemas de comunicación y la tecnología de la identificación y la autenticación. También es importante fomentar una cadena de suministro industrial europea en materia de ciberseguridad competitiva apoyando la participación de las pequeñas y medianas empresas (pymes).

Garantizar que Europa pueda mantenerse al ritmo de la competencia internacional en capacidad tecnológica cibernética depende también de nuestra capacidad para impulsar la innovación de vanguardia mediante instrumentos tanto nacionales como de la Unión, por ejemplo el Consejo Europeo de la Innovación.

Facilitar la cooperación civil-militar en el desarrollo de capacidades de ciberdefensa, reforzar la base industrial y tecnológica de la defensa europea [10]y contribuir a la autonomía estratégica de la UE también en el ámbito del ciberespacio, cuando y donde sea necesario y con los socios siempre que sea posible**,**

La AED, la Comisión y los Estados miembros:

- procurarán que se alcancen sinergias de los esfuerzos en materia de I+T en el sector militar con los programas civiles de Investigación y Desarrollo, en particular con los relativos a innovaciones de vanguardia, y tendrán en cuenta la dimensión de la ciberseguridad y la ciberdefensa cuando emprendan la acción preparatoria sobre investigación en materia de defensa;
- intercambiarán los planes de investigación en ciberseguridad (por ejemplo los programas estratégicos de investigación de la Agencia Europea de Defensa), así como las hojas de ruta y medidas resultantes; a tal fin se desarrollará un programa de investigación en ciberdefensa en estrecha cooperación con la Comisión y los Estados miembros.
- contribuirán a mejorar la integración de las dimensiones de ciberseguridad y ciberdefensa en los programas que tengan una dimensión de seguridad y defensa de doble uso, como por ejemplo el programa de investigación sobre la gestión del tráfico aéreo en el contexto del Cielo Único Europeo (SESAR).

[10] Comunicación «Hacia un sector de seguridad y defensa más competitivo y eficiente» (COM (2013) 542).

La Comisión:

- estudiará la creación de un Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad con una Red de Centros Nacionales de Coordinación para mejorar las capacidades industriales y tecnológicas en ciberseguridad y aumentar la competitividad de la industria europea de ciberseguridad, garantizando la complementariedad y evitando duplicaciones dentro de la red de centros de competencia en ciberseguridad y con otras agencias de la UE. El Centro deberá, entre otras cosas, mejorar la cooperación entre las aplicaciones y tecnologías del ámbito civil y de la defensa; para ello trabajará en estrecha colaboración y con plena complementariedad con la Agencia Europea de Defensa en materia de ciberdefensa;
- apoyará el desarrollo de ecosistemas industriales y de agrupaciones empresariales innovadoras que cubran la totalidad de la cadena de valor, aprovechando para ello el conocimiento del mundo académico, la innovación de las pymes y la producción industrial.

La Comisión, en cooperación con los Estados miembros:

- estudiará las cuestiones de ciberdefensa en las convocatorias para la Acción preparatoria sobre investigación en materia de defensa;
- estudiará la ciberdefensa entre los temas que se tratarán en el Fondo Europeo de Defensa;
- apoyará la coherencia de las actuaciones de la UE con el fin de garantizar que los aspectos de política y técnicos de la ciberprotección de la UE sigan figurando a la cabeza de la innovación tecnológica y estén armonizados en toda la UE (análisis de ciberamenazas y evaluación de capacidades, iniciativas de «seguridad desde el diseño», gestión de la dependencia para el acceso a la tecnología, etc.).

5. Mejorar las posibilidades de educación, formación y ejercicios

Para mejorar la preparación ante las ciberamenazas y desarrollar una cultura común de ciberdefensa en la UE, que también beneficie a las misiones y operaciones de la UE, se necesita mejorar y aumentar las posibilidades de formación en ciberdefensa. Es crucial que los presupuestos de educación y formación se utilicen de forma eficiente y que se logre, al mismo tiempo, la mayor calidad posible. La puesta en común de la educación y formación en materia de ciberdefensa a escala europea tendrá una importancia clave.

La Escuela Europea de Seguridad y Defensa (EESD), el SEAE, la AED, la Comisión y los Estados miembros:

- basándose en el análisis de las necesidades de formación en materia de ciberdefensa de la AED y en las experiencias adquiridas por la EESD en la formación impartida en materia de ciberseguridad, establecerán cursos de formación y educación PCSD para diferentes públicos, en particular el SEAE, el personal de las misiones y operaciones PCSD y los funcionarios de los Estados miembros, lo cual debería también solucionar el problema de cómo conservar al personal cualificado a corto, medio y largo plazo;
- Propondrán el establecimiento de un diálogo en materia de ciberdefensa sobre normas de formación y certificación con los Estados miembros, las instituciones de la UE, terceros países y otras organizaciones internacionales, así como con el sector privado;
- colaborarán con el sector privado europeo de proveedores de formación, y con las instituciones académicas, para aumentar las competencias y cualificaciones del personal que participa en las misiones y operaciones de la PCSD.

La EESD:

- seguirá desarrollando la plataforma de educación, formación, evaluación y ejercicio en materia de cibernética creada por la EESD;
- creará sinergias con los programas de formación de otras partes interesadas, como ENISA, Europol, la Escuela Europea de Policía (CEPOL) y el Centro de Excelencia para la Ciberdefensa Cooperativa de la OTAN;
- estudiará la posibilidad de crear programas conjuntos EESD-OTAN sobre ciberdefensa abiertos a todos los Estados miembros de la UE, con el fin de fomentar unos hábitos compartidos en materia de ciberdefensa.

La Comisión:

- valorará las opciones para aumentar las posibilidades de formación y educación en los Estados miembros que determine la plataforma de educación, formación, evaluación y ejercicio en materia de cibernética.

La AED:

- desarrollará nuevos cursos de la AED en colaboración con la EESD para cumplir los requisitos de educación, formación y ejercicios en ciberdefensa de los Estados miembros;
- apoyará la plataforma de educación, formación, evaluación y ejercicio en materia de cibernética, entre otras cosas mediante la integración progresiva de módulos sobre dichas materias elaborados en el marco de la AED.

El SEAE y los Estados miembros:

- seguirán los mecanismos de certificación establecidos por la EESD para los programas de formación en estrecha cooperación con los servicios correspondientes de las instituciones, organismos y agencias de la UE, basándose en las normas y conocimientos de que se dispone; considerarán la posibilidad de crear módulos específicos de ciberseguridad en el marco de la iniciativa Erasmus militar.

Es necesario mejorar las oportunidades para que los diversos agentes militares y civiles encargados de la PCSD realicen ejercicios en materia de ciberdefensa. Los ejercicios conjuntos sirven como instrumento para impulsar un conocimiento y comprensión comunes de la ciberdefensa. Ello permitirá a las fuerzas nacionales mejorar su grado de preparación para actuar en un entorno multinacional. La organización de ejercicios comunes de ciberdefensa aumentará también la interoperabilidad y la confianza mutua.

El SEAE, la AED, el CERT-UE y los Estados miembros se centrarán en promover los elementos relativos a la ciberdefensa en la PCSD y otros ejercicios, como por ejemplo:

- integrar una dimensión de ciberdefensa en los supuestos de ejercicio existentes para *MILEX* y *MULTILAYER*;
- organizar regularmente ejercicios estratégicos y políticos como *CYBRID 2017*, en coordinación con el ejercicio paralelo y coordinado (PACE) dirigido por la UE, y ejercicios técnicos y operativos como *DEFNET*;
- impulsar, según proceda, un ejercicio específico en materia de ciberdefensa de la PCSD de la UE y estudiar la posible coordinación con otros ejercicios paneuropeos en la materia, como por ejemplo *CyberEurope*, organizado por ENISA;
- seguir participando en otros ejercicios multinacionales de ciberdefensa, como *Locked Shields*;
- invitar a los socios internacionales pertinentes, como la OTAN, a participar en los ejercicios de conformidad con el marco estratégico de ejercicios de la UE;
- organizar ejercicios regulares basados en el conjunto de instrumentos de ciberdiplomacia en los que los Estados miembros de la UE puedan practicar las respuestas a actividades cibernéticas malintencionadas.

6. Incrementar la cooperación con los socios internacionales pertinentes

En el marco de la cooperación internacional, es necesario garantizar el diálogo con los socios internacionales, en concreto la OTAN y otras organizaciones internacionales, para contribuir a impulsar unas capacidades eficaces en materia de ciberdefensa. Deberá propiciarse una mayor participación en las labores realizadas en el marco de la Organización para la Seguridad y la Cooperación en Europa (OSCE) y de las Naciones Unidas (ONU), con vistas a presentar un marco estratégico para la prevención de conflictos, la cooperación y la estabilidad en el ciberespacio.

Existe la voluntad política en la UE de reforzar la cooperación con la OTAN en materia de ciberdefensa, mediante el desarrollo de capacidades en ciberdefensa sólidas y resilientes, tal y como exige la declaración conjunta firmada por el presidente del Consejo Europeo, el presidente de la Comisión Europea y el secretario general de la Organización del Tratado del Atlántico Norte, en Varsovia el 8 de julio de 2016. Consultas regulares entre el personal de ambas instituciones, sesiones informativas transversales y posibles reuniones entre el Grupo Político-Militar y los correspondientes comités de la OTAN ayudarán a evitar duplicaciones innecesarias y a garantizar la coherencia y complementariedad de esfuerzos, en consonancia con el mencionado marco.

El SEAE y la AED, junto con los Estados miembros, impulsarán en mayor medida la cooperación en materia de ciberdefensa entre la UE y la OTAN, respetando plenamente el marco institucional y la autonomía del proceso decisorio de estas dos organizaciones:

- intensificarán las actividades en curso en el marco de la puesta en práctica de la declaración conjunta del presidente del Consejo Europeo, el presidente de la Comisión Europea y el secretario general de la Organización del Tratado del Atlántico Norte;
- intercambiarán las mejores prácticas en la gestión de crisis y en la ciberdefensa de misiones y operaciones militares y civiles;
- procurarán que los requisitos relativos al desarrollo de capacidades de ciberdefensa sean coherentes en caso de producirse solapamientos, especialmente en el desarrollo de capacidades de ciberdefensa a largo plazo;
- Utilizarán en mayor medida el marco de cooperación de la AED con el Centro de Excelencia para la Ciberdefensa Cooperativa de la OTAN como plataforma inicial para una colaboración más intensa en proyectos multinacionales de ciberdefensa, basándose en las evaluaciones adecuadas.

La EESD, el SEAE y la AED:

- mejorarán la cooperación en relación con los conceptos de formación y educación sobre ciberdefensa, así como con los ejercicios al respecto;
- garantizarán la participación recíproca del personal en los ejercicios, de conformidad con el marco acordado.

CERT-UE:

- seguirá explotando el acuerdo técnico entre el CERT de la UE y el NCIRC (Capacidad de respuesta ante incidentes informáticos de la OTAN) con el fin de mejorar el conocimiento de las situaciones, el intercambio de información y los mecanismos de alerta temprana y prever amenazas que pudieran afectar a ambas organizaciones.

Con respecto a otras organizaciones internacionales y a los socios internacionales pertinentes de la UE, el SEAE y los Estados miembros, cuando proceda:

- seguirán de cerca la evolución estratégica y mantendrán consultas sobre asuntos de ciberdefensa con sus socios internacionales (organizaciones internacionales y terceros países);
- explorarán las posibilidades de cooperación en asuntos de ciberdefensa, inclusive con terceros países que participen en misiones y operaciones PCSD;
- promoverán en las organizaciones internacionales pertinentes, en particular en las Naciones Unidas, la OSCE y el Foro Regional de la ASEAN, la aplicación, en el ciberespacio, del Derecho internacional en vigor, especialmente la Carta de las Naciones Unidas en su totalidad, así como la creación y ejecución de normas universales no vinculantes que definan un comportamiento responsable de los Estados y medidas de creación de confianza de ámbito regional entre los Estados para reforzar la transparencia y reducir el riesgo de una percepción errónea del comportamiento de un Estado.

La Comisión y el SEAE:

- cuando sea pertinente, apoyarán la creación de capacidades cibernéticas para los socios de la UE mediante el Instrumento modificado en pro de la Estabilidad y la Paz.

Actuación consecutiva

En el contexto del trabajo de coordinación realizado por el SEAE de la aplicación del marco político de ciberdefensa, el SEAE, la AED y la Comisión deberán presentar al Grupo Político-Militar, con la participación de los miembros del Grupo Horizontal «Cuestiones Cibernéticas», y al Comité Político y de Seguridad un informe anual sobre el desarrollo de los trabajos que trate los seis puntos expuestos anteriormente, con el fin de evaluar la aplicación del marco. También se hará una presentación oral cada seis meses.

Es esencial que, a medida que evolucionan las diversas amenazas cibernéticas, se establezcan nuevos requisitos en materia de ciberdefensa, que se incluyan a continuación en el marco político de ciberdefensa de la UE. La próxima revisión del marco político de ciberdefensa debería presentarse, a más tardar, a mediados de 2022, previa consulta a los Estados miembros.