Francisco Pérez Bes
Socio de Derecho Digital en Ecix Tech
Doctorando en Derecho Público por la Universidad de Salamanca
Profesor de Derecho de la Ciberseguridad en la Universidad Francisco de Vitoria (UFV)

LA REGULACIÓN DE UNA RESERVA DE CIBERSEGURIDAD. UNA VISIÓN DESDE EL REGLAMENTO EUROPEO DE CIBERSOLIDARIDAD

LA REGULACIÓN DE UNA RESERVA DE CIBERSEGURIDAD. UNA VISIÓN DESDE EL REGLAMENTO EUROPEO DE CIBERSOLIDARIDAD

Resumen: El nuevo Reglamento europeo de Cibersolidaridad se aprobó en marzo de 2024. Como una de sus principales novedades está la de la creación de la figura de reserva de ciberseguridad, como recurso que, junto a la red europea de SOC y a los proveedores de seguridad gestionada, deben cooperar en la gestión de incidentes de ciberseguridad de especial trascendencia. Gracias a ello se refuerza el concepto de escudo de ciberseguridad europeo (*european cyber shield*) que es uno de los objetivos prioritarios de la Unión Europea para los próximos años. Esta propuesta va a requerir un diseño y un desarrollo específico, que puede concluir con otras propuestas individuales que puedan plantear otros Estados miembros, como en el caso de Francia y su *réserve citoyenne de cyberdéfense*. En una línea similar, España propuso en el año 2021 un proyecto de ciber reserva que, ante su falta de aprobación política, ha vuelto a presentarse a la Comisión de Defensa del Congreso de los Diputados el pasado 8 de marzo de 2024.

Abstract: The new European Regulation on Cybersolidarity was approved on March 2024. As one of its main novelties is the introduction of a cybersecurity reserve, as a resource that, together with the European network of SOCs and managed security providers, must cooperate in the management of cybersecurity incidents of particular importance. This should reinforce the concept of a European cybersecurity shield, which is one of the priority objectives of the European Union for the coming years. This proposal will require specific design and development, which may be concluded with other individual proposals that may be put forward by other Member States, as in the case of France and its *réserve citoyenne de cyberdéfense*. In a similar vein, Spain proposed a cyber reserve project in 2021, which, in the absence of political approval, was resubmitted to the Defence Committee of the Congress of Deputies on 8 March 2024.

Palabras clave: Cibersolidaridad, ciberreserva, reserva de ciberseguridad, ciberescudo.

Keywords: Cybersolidarity, cyberreserve, reserve of cybersecurity, cyber shield.

ABREVIATURAS

Art.: Artículo

BOCG: Boletín Oficial de las Cortes Generales

BOE: Boletín Oficial del Estado

CE: Comisión Europea

CERT: Computer Emergency Response Team

CSIRT: Computer Security Incident Reaction Team

DOUE: Diario Oficial de la Unión Europea

ENISA: Agencia de la Unión Europea para la Ciberseguridad

GC: Guardia Civil

INCIBE: Instituto Nacional de Ciberseguridad de España

PNL: Proposición no de Ley

SOC: Centro de Operaciones de Seguridad

UE: Unión Europea

1. INTRODUCCIÓN: UNA RESERVA DE CIBERSEGURIDAD PARA LA CIBERSOLIDARIDAD.

En fecha 22 de marzo de 2024, la prensa española publicaba un artículo que llevaba por título el de "la UE pide a la ciudadanía prepararse para afrontar *todos los peligros*", un artículo en el que trataba la amenaza militar a la que se enfrentan los ciudadanos europeos en un plazo de tiempo corto (se habla de un conflicto armado con Rusia para 2026). Además, se afirmaba que "la guerra va más allá del lanzamiento de misiles y la sociedad debe ser consciente, advierten en un cambio de lenguaje claro. Hablar de la preparación de la sociedad civil marca un cambio de patrón en la UE". Dicho artículo añade una serie de datos que impactan directamente en la ciberseguridad continental, cuando alerta que "la UE, consciente de su vulnerabilidad, teme ciberataques que paralicen los servicios, agresiones a infraestructuras civiles -como instalaciones energéticas o cables de telecomunicaciones- y campañas masivas de desinformación"[1].

Unos días antes, la ministra de Defensa española, Margarita Robles, era entrevistada en ese mismo medio, donde respondía a la pregunta acerca de si podía considerarse real la amenaza de guerra, ante la llamada de varios líderes europeos al rearme de la Unión Europea. En dicha entrevista, destacaba que "la amenaza es total y absoluta. […] Europa tiene que ser consciente de que el peligro está muy cerca; no es una pura hipótesis, es real. Los países fronterizos con Rusia lo perciben muy bien; quizá los del sur no tenemos esa conciencia, pero la civilización puede ser atacada por personas sin escrúpulos como Putin"[2].

Poco más de un año antes, en concreto el 10 de noviembre de 2022, la Comunicación conjunta sobre una política europea en ciberdefensa ya anunciaba una iniciativa sobre cibersolidaridad[3], en la que se identificaban una serie de objetivos. Entre ellos, se incluía la creación de capacidades específicas de ciberdefensa europeas para hacer frente a incidentes de ciberseguridad considerados significativos por su alto nivel de gravedad.

En el citado documento ya se contemplaba que tales recursos debían desarrollarse sobre el refuerzo de capacidades de detección y respuesta ante ciberataques, promoviendo una infraestructura europea de centros de operaciones de seguridad (comúnmente conocidos como SOC, siglas en inglés para *Security Operations Centres*) que debía dar apoyo gradual a la construcción de un de cuerpo de reserva de ciberseguridad a nivel europeo constituida por proveedores privados de seguridad gestionada. Estos proveedores serán designados como tales por su nivel de confiabilidad, y deberán tener como objetivo el de reforzar principalmente la seguridad de las infraestructuras críticas ante incidentes cibernéticos de alto impacto.

---

[1] Diario El País (2024, marzo). *La UE pide a la sociedad preparase para afrontar todos los peligros y un panorama de amenazas cambiante.*
https://elpais.com/internacional/2024-03-21/la-ue-pide-a-la-sociedad-prepararse-para-afrontar-todos-los-peligros-y-un-panorama-de-amenazas-cambiante.html

[2] Radio Televisión Española (2024, marzo). *La amenaza de un ataque de Rusia es absoluta.*
https://www.rtve.es/play/videos/fin-de-semana-24h/robles-amenaza-ataque-rusia-absoluta/16019094/

[3] Comisión Europea (2022, 10 de noviembre). *Ciberdefensa: la UE impulsa medidas contra las ciberamenazas* [nota de prensa]
https://ec.europa.eu/commission/presscorner/detail/es/ip_22_6642

Recientemente, en marzo de 2024, siguiendo con los plazos de tramitación de la citada iniciativa, la Unión Europea (UE) aprobó, dentro de su paquete de medidas legislativas en materia de ciberseguridad, el *Cybersolidarity Act*: un Reglamento sobre cibersolidaridad que tiene por objeto reforzar las capacidades en la Unión para detectar, prepararse y responder a amenazas y ataques de ciberseguridad significativos y a gran escala[4]. Estas capacidades también podrán, en su caso, ser requeridas por terceros países afectados por ciberincidentes de extrema magnitud, en el caso de que mantengan suscrito con la Unión Europea algún tipo de acuerdo de colaboración a estos efectos[5].

Dentro de las medidas que contempla esta nueva norma destaca el de la creación de una reserva de ciberseguridad que, según afirma la propia Comisión Europea, "consistirá en servicios de respuesta a incidentes de proveedores de servicios privados («proveedores de confianza»), que podrán desplegarse a petición de los Estados miembros o de las instituciones, organismos y agencias de la Unión para ayudarles a abordar incidentes de ciberseguridad significativos o a gran escala"[6].

Dicho con otras palabras, el citado Reglamento prevé la creación de una ciberreserva europea, consistente en servicios de prevención y respuesta ante incidentes cibernéticos por parte de proveedores de confianza, seleccionados de conformidad con los criterios establecidos en el mismo Reglamento. Entre los posibles usuarios de los servicios de dicha Reserva, se encuentran las autoridades de gestión de crisis cibernéticas y los CSIRT de los Estados miembros, así como las instituciones, órganos y otros organismos de la Unión.

Adicionalmente, el documento considera que debe ser la Comisión Europea la responsable de la constitución de la Reserva de Ciberseguridad de la UE, y podrá confiar total o parcialmente a la Agencia europea de ciberseguridad (ENISA) la financiación, el funcionamiento y la gestión de dicho órgano[7].

En este sentido, el Considerando 33 de la propuesta inicial de Reglamento reflejaba esta conveniencia de contar con una reserva de ciberseguridad, teniendo como fin último el de la creación de un ciberescudo europeo ("*cyber shield*") que refuerce la seguridad de las infraestructuras estratégicas de los Estados miembros y, por tanto, los de la Unión Europea en su integridad[8]:

---

[4] Vid. Art. 1.1 de la Propuesta de Reglamento: "This Regulation lays down measures to strengthen capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents, in particular through the following actions: […]",

[5] *to gradually build an EU-level cybersecurity reserve with services from trusted private providers and to support testing of critical entities.*

[6] Comisión Europea (2024, marzo). *La Ley de Ciber Solidaridad de la UE.* https://digital-strategy.ec.europa.eu/es/policies/cyber-solidarity

[7] *For the purpose of implementing the proposed incident response actions, this Regulation establishes an EU Cybersecurity Reserve, consisting of incident response services from trusted providers, selected in accordance with the criteria laid down in this Regulation. Users of the services from the EU Cybersecurity Reserve shall include Member States' cyber crisis management authorities and CSIRTs and Union institutions, bodies and agencies. The Commission shall have overall responsibility for the implementation of the EU Cybersecurity Reserve and may entrust, in full or in part, ENISA with the operation and administration of the EU Cybersecurity Reserve.*

[8] Traducción libre: Los servicios de la Reserva de Ciberseguridad de la UE deben servir para apoyar a las autoridades nacionales en la prestación de asistencia a las entidades afectadas que operan en sectores críticos o muy críticos como complemento de sus propias acciones a nivel nacional. Al solicitar apoyo de

> *The services from the EU Cybersecurity Reserve should serve to support national authorities in providing assistance to affected entities operating in critical or highly critical sectors as a complement to their own actions at national level. When requesting support from the EU Cybersecurity Reserve, Member States should specify the support provided to the affected entity at the national level, which should be taken into account when assessing the Member State request. The services from the EU Cybersecurity Reserve may also serve to support Union institutions, bodies and agencies, under similar conditions.*

Más concretamente, el capítulo II de la propuesta de Reglamento que lleva por título "el ciberescudo europeo", incluye un artículo 3 cuyo apartado primero se refiere al establecimiento de esta figura con la siguiente redacción:

> *1. An interconnected pan-European infrastructure of Security Operations Centres ('European Cyber Shield') shall be established to develop advanced capabilities for the Union to detect, analyse and process data on cyber threats and incidents in the Union. It shall consist of all National Security Operations Centres ('National SOCs') and Cross-border Security Operations Centres ('Cross-border SOCs').*

Si atendemos al articulado de la tan citada *Cybersolidarity Act,* son los artículos 12 y siguientes los que regulan la constitución, funcionamiento y requisitos que deben cumplir los proveedores que constituyan la reserva de ciberseguridad en el sentido antes expuesto.

Finalmente, hay que tener en cuenta que la aprobación y posterior entrada en vigor de este nuevo Reglamento de cibersolidaridad, supondrá la modificación de determinadas normas europeas como , por ejemplo, el Programa Europa Digital[9].

Como ejemplo de algunos de los cambios que se proponen en la citada norma, cabe destacar la propuesta de inclusión, en el actual artículo 6 del Reglamento 2021/694, del siguiente texto:

> *(aa) support the development of an EU Cyber Shield, including the development, deployment and operation of National and Cross-border SOCs platforms that contribute to situational awareness in the Union and to enhancing the cyber threat intelligence capacities of the Union';*

> *'(g) establish and operate a Cyber Emergency Mechanism to support Member States in preparing for and responding to significant cybersecurity incidents, complementary to national resources and capabilities and other forms of support*

---

la Reserva de Ciberseguridad de la UE, los Estados miembros deberán especificar el apoyo prestado a la entidad afectada a nivel nacional, que deberá tenerse en cuenta al evaluar la solicitud del Estado miembro. Los servicios de la Reserva de Ciberseguridad de la UE también pueden servir para apoyar a las instituciones, organismos y agencias de la Unión, en condiciones similares.

[9] Reglamento 2021/694, del Parlamento Europeo y del Consejo de 29 de abril de 2021 por el que se establece el Programa Europa Digital y por el que se deroga la Decisión (UE) 2015/2240 https://www.boe.es/buscar/doc.php?id=DOUE-L-2021-80609

available at Union level, including the establishment of an EU Cybersecurity Reserve';

Por último, debemos diferenciar esta iniciativa de alguna otra, también planteada a este nivel de colaboración internacional. Así, por ejemplo, encontramos la presentada en 2023 por parte del exsenador español José Cepeda, quien recibió el encargo de la Unión Interparlamentaria (UIP) de elaborar un informe sobre el cibercrimen, Ciberataques y delitos cibernéticos, nuevas amenazas a la seguridad global. En este trabajo, se propuso la creación de un nuevo cuerpo de "cibercascos azules" para proteger, a través de la ONU, a los ciudadanos del ciberterrorismo y la ciberdelincuencia. Por su parte, la Unión Europea continúa desarrollando actuaciones centradas en la ciberseguridad y en la lucha contra la ciberdelincuencia[10].

Según se afirma[11], dicha propuesta ha obtenido un apoyo unánime y el reconocimiento mundial, si bien se espera poder avanzar hacia su consolidación en la próxima cumbre mundial, prevista para 2024.

2. FUNCIONES DE UNA CIBERRESERVA EN LA ERA DIGITAL.

En la era de la sociedad digital actual, cada vez más hiperconectada, el planteamiento de creación de un cuerpo de apoyo externo a las propias estructuras y recursos públicos se ha fundamentado tradicionalmente en el espíritu de colaboración público-privada, centrada en la resolución técnica de incidentes de ciberseguridad.

Una de las principales funciones de este soporte cualificado, centrado en aspectos eminentemente técnicos, sería la de complementar las capacidades públicas existentes, las cuales -por limitaciones presupuestarias, de conocimientos o de recursos- pueden necesitar de un refuerzo adicional en determinados momentos. Y, a estos efectos, se considera que tal soporte puede ser prestado de forma eficaz desde un sector privado, que presumiblemente dispone de numerosas capacidades técnicas, de conocimiento y experiencia, entre otras. Todo ello puede coadyuvar a la gestión adecuada de determinados incidentes de ciberseguridad, especialmente los más complejos.

Para ello, el planteamiento de una colaboración eficaz requiere diseñar un cuerpo de profesionales cuyo alto grado de flexibilidad y experiencia profesional permitan apoyar activamente la gestión de incidentes específicos y de situaciones de emergencia que, por su gravedad, podrían sobrepasar las capacidades de las entidades afectadas o de las autoridades competentes.

Este sería el caso de los Centros de Operaciones de Seguridad (SOC), tal y como recoge la propuesta de Reglamento de cibersolidaridad, cuando prevé que puedan solicitar el apoyo de los proveedores de seguridad gestionada en determinados supuestos. Pero también podría serlo en el caso de los equipos de respuesta ante ciberincidentes (CSIRT),

[10] Consejo Europeo (2024, junio). *Ciberseguridad: cómo combate la UE las amenazas cibernéticas* https://www.consilium.europa.eu/es/policies/cybersecurity/

[11] https://www.escudodigital.com/expertos/entrevistas/jose-cepeda-para-funcionen-cibercascos-azules-se-necesitan-confianza-cooperacion-entre-paises_56576_102.html

a razón de lo previsto en los artículos 10 y siguientes de la comúnmente conocida como Directiva NIS 2[12].

Como es sabido, esta Directiva reserva a los CSIRT las competencias reactivas a la gestión de incidentes de ciberseguridad de especial relevancia, cuando afecten a entidades esenciales o a empresas importantes.

Con respecto a los CSIRT, la Disposición adicional novena de la Ley 34/2002, de servicios de la sociedad de la información y del comercio electrónico ya se refería a esta organización (todavía bajo la tradicional denominación de CERT), de la siguiente manera:

> 1. Los prestadores de servicios de la Sociedad de la Información, los registros de nombres de dominio y los agentes registradores que estén establecidos en España están obligados a prestar su colaboración con el CERT competente, en la resolución de incidentes de ciberseguridad que afecten a la red de Internet y actuar bajo las recomendaciones de seguridad indicadas o que sean establecidas en los códigos de conducta que de esta Ley se deriven.
>
> Los órganos, organismos públicos o cualquier otra entidad del sector público que gestionen equipos de respuesta a incidentes de seguridad colaborarán con las autoridades competentes para la aportación de las evidencias técnicas necesarias para la persecución de los delitos derivados de dichos incidentes de ciberseguridad.
>
> 2. Para el ejercicio de las funciones y obligaciones anteriores, los prestadores de servicios de la Sociedad de la información, respetando el secreto de las comunicaciones, suministrarán la información necesaria al CERT competente, y a las autoridades competentes, para la adecuada gestión de los incidentes de ciberseguridad, incluyendo las direcciones IP que puedan hallarse comprometidas o implicadas en los mismos.

Llegados a este punto, debe identificarse cuáles son los principales motivos que hacen recomendable para los países del entorno europeo disponer de una fuerza adicional, de intervención complementaria y extraordinaria, como pueda ser la de un cuerpo de ciberreservistas, en el sentido propuesto por el Reglamento de cibersolidaridad:

En primer lugar, podemos destacar el de la rápida y constante evolución de las amenazas cibernéticas que, desde la óptica de la ciberseguridad, requieren a las organizaciones llevar a cabo tareas constantes de identificación, descripción, y conocimiento actualizado de su funcionamiento e impacto.

[12] 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) nº 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148

A la vista de ello, y sabedores de que las amenazas cibernéticas evolucionan a la vez que lo hace el avance de la tecnología, la ciberreserva puede adaptarse de forma rápida y efectiva a las nuevas amenazas, tecnologías y tácticas empleadas por los atacantes.

También la dependencia funcional que las infraestructuras críticas y estratégicas tienen de la tecnología es un hecho innegable, en particular a la vista de que la resiliencia de tales infraestructuras y de los operadores que las sostienen y gestionan es fundamental para poder garantizar la continuidad de servicios esenciales y críticos.

Asimismo, un recurso como la ciberreserva permite estructurar una formación especializada para aquellos profesionales altamente cualificados y comprometidos con la defensa nacional, también en áreas consideradas "no técnicas" (inteligencia, Derecho, economía, comunicación, etc.) donde es sabida la carencia de recursos en las estructuras públicas.

A este respecto, no hay que olvidar que lo que tiene que ver con la seguridad nacional, tal y como viene definida en la Ley de Seguridad Nacional 36/2015, de 28 de septiembre[13], y en la Estrategia de Seguridad Nacional del año 2021[14], no se limita a la defensa militar tradicional, sino que también abarca la protección de la economía, la sanidad, el medioambiente y, como no, también la protección contra amenazas cibernéticas.

Así pues, a la vista de tales motivos que justifican la creación de una reserva de ciberseguridad a iniciativa del propio Estado, poder establecer una estructura de cooperación entre tal ciberreserva y el sector privado (en este caso a través de los servicios de seguridad gestionada) es esencial. Efectivamente, la mayoría de las infraestructuras y servicios críticos están en manos privadas, y son muchas las personas que, desempeñando labores profesionales en aquellas, pueden -en base a su experiencia- aportar perspectivas y conocimientos de gran utilidad a la hora de proteger las redes y sistemas, a la vez que se refuerza y mejora la coordinación con el sector privado, tal y como ya prevé la normativa de resiliencia de las entidades críticas.

3. ORÍGENES DE LA CIBERRESERVA.

La idea de configurar una fuerza de soporte técnico especializado se remonta a los mismos inicios de internet, cuando las fuerzas armadas y las agencias de inteligencia empezaron a reconocer sus carencias y limitaciones (de conocimientos y de recursos) a la hora de gestionar determinados incidentes de seguridad; mientras que el sector privado disponía de personas cuyos conocimientos y habilidades podrían resultar de gran ayuda en determinados momentos en los que la seguridad nacional pudiese verse afectada como consecuencia de algún tipo de incidente cibernético de alto impacto.

De ello pudimos ser testigos con la aparición de los conocidos como *Computer Emergency Response Teams* (o CERT, por sus siglas en inglés), surgidos a la vista de las

[13] Ley 36/2015, de 28 de septiembre, de Seguridad Nacional. https://www.boe.es/buscar/act.php?id=BOE-A-2015-10389

[14] Departamento de Seguridad Nacional (2024, junio). *Estrategia de Seguridad Nacional* https://www.dsn.gob.es/es/estrategias-publicaciones/estrategias/estrategia-seguridad-nacional-2017

necesidades de proteger las redes y sistemas de información, así como la información que en ellos se alojaba, ante las primeras amenazas que comenzaba a desarrollarse en Internet.

Ante un escenario de esta naturaleza, la agencia norteamericana DARPA (*Defence Advanced Research Projects Agency*)[15], financió un proyecto que permitiría mejorar la coordinación en las respuestas a las nuevas amenazas cibernéticas, consistente en el diseño y creación de una red de equipos técnicos especialistas en gestionar reactivamente incidentes de seguridad cibernética, a los que se denominó *Computer Emergency Reaction Teams* o, en sus siglas en inglés, CERT.

Y es que, como es sabido, la naturaleza de las amenazas cibernéticas se ha vuelto cada vez más compleja, más diversa y plural, y de que sus objetivos se han ampliado a gobiernos, empresas y ciudadanos. Esto ha llevado a la necesidad de desarrollar capacidades de respuesta cada vez más amplias y flexibles para enfrentar estas amenazas emergentes.

Uno de los hitos importantes en la evolución de la ciberreserva fue el reconocimiento de que los ciberataques pueden tener efectos devastadores en la vida civil y en la economía[16], lo que -como veremos- ha llevado a que cada vez más países hayan diseñado programas formales de ciberreservistas para proteger a la población y a los intereses nacionales.

En este sentido, la ciberreserva -tal y como lo plantea el Reglamento europeo- puede jugar un papel relevante en la seguridad nacional al proporcionar una fuerza colaborativa de respuesta altamente capacitada y adaptable, que puede movilizarse rápidamente para abordar incidentes cibernéticos y proteger las infraestructuras críticas u otros recursos que puedan verse amenazados[17]. La reserva de ciberseguridad, tal y como prevé el Reglamento de Cibersolidaridad, trabajaría en estrecha colaboración con las autoridades competentes para fortalecer las capacidades defensivas del país afectado y reducir el impacto de determinados ciberataques.

4. OBJETIVOS Y FUNCIONES DE LA CIBERRESERVA.

Una ciberreserva bien diseñada debe tener una serie de objetivos y funciones clave que guiarán su papel en el ecosistema de la ciberseguridad nacional y su contribución a la protección contra amenazas cibernéticas.

Entre los citados objetivos, como se ha indicado anteriormente, el principal es el de responder de manera eficaz a incidentes cibernéticos en aquellas circunstancias en las que sea conveniente disponer de recursos adicionales que permitan garantizar una mejor y más eficiente gestión de una situación de crisis nacional, derivada de un incidente de esta naturaleza.

---

[15] Darpa.mil

[16] Pérez Bes, F. (2022) *Los ciberataques en la empresa cotizada y su impacto en el valor de las acciones.* Fundación Esys: https://fundacionesys.com/es/los-ciberataques-en-la-empresa-cotizada-y-su-impacto-en-el-valor-de-las-acciones/

[17] Consejo de Europa (2023, 20 de diciembre). Reglamento de Cibersolidaridad: los Estados miembros acuerdan una posición común para reforzar las capacidades de ciberseguridad en la UE: https://www.consilium.europa.eu/es/press/press-releases/2023/12/20/cyber-solidarity-act-member-states-agree-common-position-to-strengthen-cyber-security-capacities-in-the-eu/

Asimismo, la ciberreserva tiene la obligación de colaborar con entidades gubernamentales, lo que supone que este cuerpo se debe poner al servicio de los poderes públicos en momentos de alta excepcionalidad, para garantizar una respuesta más eficiente frente a ciberataques masivos y, en consecuencia, reforzar la protección de los intereses nacionales.

Para ello, los reservistas en ciberseguridad deben estar capacitados para colaborar en la detección, análisis y mitigación de ciberataques de alto impacto, tal y como requiere el citado Reglamento de Cibersolidaridad, que exige que los profesionales que compongan la reserva de ciberseguridad tengan conocimientos técnicos altamente especializados.

En este sentido, la propuesta de Reglamento parece adolecer de una carencia a la hora de exigir -únicamente- capacitación técnica en la respuesta a ciberincidentes, olvidando la relevancia que tienen las habilidades y conocimientos de su gestión, especialmente a la hora de colaborar en la minimización de los daños, en la restauración de la normalidad en los sistemas afectados y de la defensa de los derechos de los ciudadanos y la reputación de la entidad afectada.

Esta necesidad supone una oportunidad para los países europeos a la hora de fomentar esas capacitaciones, tanto directamente desde los poderes públicos (en España, por ejemplo, con iniciativas como el *Summer Bootcamp* del INCIBE[18], la *National Cyberleague* de la Guardia Civil[19], o C1b3rw4ll de la Policía Nacional[20]), como a través de programas diseñados y realizados por las propias empresas que, voluntariamente, quieran colaborar con una iniciativa como la de la ciberreserva.

Llegados a este punto, tampoco hay que olvidar que otro objetivo importante de la ciberreserva será el de promover la concienciación en ciberseguridad entre la población en general, y las empresas privadas en particular. Con respecto a este extremo, los reservistas pueden desempeñar un papel activo en la educación sobre buenas prácticas de seguridad cibernética (concepto que la Directiva NIS2 califica de “ciberhigiene”), y en la prevención de incidentes por medio de la concienciación y la sensibilización en sus organizaciones, pero también en centros educativos y, especialmente, en colectivos vulnerables, como pueden ser los niños o las personas mayores.

Así las cosas y a la vista de lo anterior, puede concluirse que no parece excluyente un sistema de reserva de ciberseguridad como el que plantea el Reglamento europeo de Cibersolidaridad (a través de la red de SOC) con la existencia de un cuerpo de profesionales especializados en ciberseguridad, que no desempeñen necesariamente su labor en proveedores de seguridad gestionada, pero que, en determinados momentos, puedan resultar útiles durante el proceso de gestión de un incidente de ciberseguridad de gravedad relevante.

[18] https://www.incibe.es/en/events/summer-bootcamp
[19] https://www.nationalcyberleague.es/
[20] https://c1b3rwall.policia.es/

5. BENEFICIOS DE CONTAR CON UNA CIBERRESERVA.

La creación y el mantenimiento de una ciberreserva pueden aportar una serie de beneficios significativos en el ámbito de la ciberseguridad nacional y la protección contra amenazas cibernéticas relacionadas con la resiliencia del Estado.

A nivel operativo, donde la capacidad de respuesta es clave en la detección y gestión de un incidente de un alto nivel de gravedad, la ciberreserva deberá ser un recurso con un alto nivel de disponibilidad para actuar en momentos de urgencia y de capacidad de gestión. Una inmediata disponibilidad permitirá una movilización rápida y efectiva de cara a responder ante incidentes cibernéticos, logrando minimizar el impacto de los ataques y acelerar la recuperación de sistemas y servicios afectados.

En caso de que ocurra una crisis o un ataque cibernético de gran magnitud, la ciberreserva proporciona un respaldo valioso para reforzar los esfuerzos de seguridad nacional. Su presencia puede ayudar a mitigar los efectos de un incidente y asegurar la continuidad de las operaciones críticas del país.

Además, debe tratarse de un recurso que aporte calidad, complementando las capacidades existentes en ciberseguridad del Estado. Esto es, que su enfoque especializado en amenazas cibernéticas y su experiencia en tecnologías de seguridad permitan abordar desafíos que excedan los recursos habituales disponibles.

Este valor añadido se aporta con un alto grado de flexibilidad y adaptabilidad, en tanto en cuanto la ciberreserva está compuesta por voluntarios provenientes de diversas áreas profesionales, lo que ofrece una gran diversidad de habilidades y conocimientos. Esta diversidad permite adaptarse a diferentes situaciones y abordar una amplia gama de amenazas cibernéticas de manera efectiva, no sólo en el aspecto exclusivamente técnico, sino también en otros tales como el jurídico, económico, sociológico, de comunicación, psicológico, etc.

Además, la ciberreserva puede fomentar una mayor colaboración entre el sector público y privado en materia de ciberseguridad, ya que al reclutar a especialistas del sector privado, se establecen vínculos que permiten compartir conocimientos y mejores prácticas, lo que mejora la seguridad en el ámbito empresarial.

A nivel de su composición, esta iniciativa ofrece a los ciudadanos la oportunidad de contribuir, con sus habilidades y conocimientos, a la protección de la seguridad nacional y de las infraestructuras críticas del país. Esta participación ciudadana en temas de ciberseguridad puede, además, fortalecer el sentido de pertenencia y responsabilidad hacia la protección de la nación.

Ser parte de la ciberreserva también ofrece a los reservistas la oportunidad de desarrollar sus habilidades técnicas, acceder a programas de formación avanzada y establecer conexiones estructuradas con otros profesionales de la ciberseguridad, tanto en el ámbito gubernamental como en el privado.

En resumen, la ciberreserva se erige en una iniciativa regulatoria que puede aportar beneficios relevantes en la ciberseguridad nacional y europea, incluyendo una respuesta rápida y efectiva ante incidentes, el aumento de capacidades en ciberseguridad,

la colaboración con el sector privado, la participación ciudadana en la seguridad nacional y el desarrollo profesional de los reservistas, etc.

Sin duda, estos beneficios hacen de la ciberreserva una herramienta valiosa para fortalecer la resiliencia y protección del país en el ciberespacio.

6. LA PROPUESTA DE CIBERRESERVA EN ESPAÑA.

En España, el 25 de marzo de 2020 se presentó una Proposición no de Ley (PNL) que tenía por objeto la constitución de una ciberreserva, bajo el título de "Proposición no de Ley relativa a la creación y regulación de la Reserva Estratégica de talento en ciberseguridad dependiente del Ministerio de Defensa para evitar los ciberataques a las instituciones en situaciones de crisis" [21].

El 21 de abril de 2021, la Comisión de Defensa acordó aprobar la citada proposición, instando al Gobierno a[22]:

> 1. Estudiar la creación de una reserva estratégica de talento en ciberseguridad, con componente civil y militar, que permita reforzar las capacidades del Ministerio de Defensa en apoyo de sus necesidades dentro del ámbito específico de la ciberdefensa, bajo la selección de personas que por su experiencia y conocimientos técnicos o de otra índole mejoren las capacidades existentes.
> 2. Estudiar las posibilidades del modelo de adscripción bajo el cumplimiento de los criterios y condiciones que se determinen, que permita compartir con empresas privadas la retención de este talento. Considerar como referencia de adscripción el sistema actual de "Reservistas Voluntarios" de las Fuerzas Armadas.
> 3. Considerar como referencia de adscripción el sistema actual de "Reservistas Voluntarios de las Fuerzas Armadas."

Con respecto a dicha iniciativa, en el Diario del Congreso[23], de fecha 21 de abril de 2021 (número de expediente 161/000461), el Grupo Parlamentario Popular en dicha Cámara (Sr. Callejas Cano) presentó una nueva propuesta, en forma de PNL, relativa a la creación y regulación de la reserva estratégica de talento en ciberseguridad dependiente del Ministerio de Defensa para evitar los ciberataques a las instituciones en situaciones de crisis.

Entre los argumentos expuestos para el debate de dicha proposición, destacan una serie de datos relativos a la situación de los recursos actuales del Mando Conjunto

[21] Comisión de Defensa del Congreso de los Diputados, número de expediente 161/000461
[22] Boletín Oficial de las Cortes Generales (BOCG) de 20 de mayo de 2021, número 276: https://www.congreso.es/public_oficiales/L14/CONG/BOCG/D/BOCG-14-D-276.PDF#page=5
[23] Boletín Oficial de las Cortes Generales (2021, 21 de abril). *Diario de Sesiones del Congreso de los Diputados*. https://www.congreso.es/es/web/guest/busqueda-de-publicaciones?p_p_id=publicaciones&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&_publicaciones_mode=mostrarTextoIntegro&_publicaciones_legislatura=XIV&_publicaciones_id_texto=(DSCD-14-CO-367.CODI.)#(P%C3%A1gina7)

del Ciberespacio, creado el 27 de julio de 2020, y que posee algo más de doscientos efectivos y activa unos quince reservistas voluntarios al año, según se afirma.

También el aspecto de la edad de los voluntarios se presenta como un elemento relevante a la hora de analizar un modelo de ciberreserva eficiente y sostenible. A este respecto, la información facilitada en dicha intervención parlamentaria sostiene que:

> *En el máster en Data Science de la Universidad Politécnica de Madrid, la media de edad del cuadro de profesores es de tan solo treinta y tres años. Actualmente, el modelo de reserva voluntaria en España, tal y como está planteado, favorece la experiencia frente al talento o el conocimiento. Es matemáticamente imposible que ninguno de los perfiles que puedan solicitarse para ciberdefensa logre acceder a la condición de reservista voluntario, por el mero hecho del hándicap que supone su juventud.*
>
> *Según se indica el desarrollo de las capacidades de ciberdefensa exige un 80 % de talento frente a un 20 % de experiencia, por lo que se propone modificar el modelo de captación de reservistas voluntarios, a los efectos de poder dar entrada al talento joven que, en el caso de perfiles técnicos, son más numerosos.*

Este planteamiento político concluye que:

> *La ciberseguridad ha de ser transversal en todas las Fuerzas Armadas, como lo es la sanidad también. Se debería explorar la creación de un cuerpo o arma específica a semejanza de unos cuerpos comunes que se apliquen a los tres ejércitos. Si bien esta sería la solución más fácil, otras opciones podrían ser la creación de una especialidad única en ciberdefensa para las Fuerzas Armadas o plantear realmente la creación de un cuarto ejército, el cíber.*

A la iniciativa descrita se presentaron dos enmiendas, una por parte del grupo parlamentario VOX y otra desde el grupo parlamentario socialista. También Ciudadanos y Podemos intervinieron en el turno de palabra para dar su opinión al respecto.

Con respecto a la primera (VOX), fue una enmienda de modificación a tal PNL, en el sentido de complementar su propuesta para resaltar la necesidad de incrementar los créditos asignados a la finalidad de la lucha contra los ciberataques desde una ciberreserva, lo que se hizo a través de los siguientes argumentos:

> *La reserva voluntaria sería, en efecto, una excelente solución. Tan solo hemos querido clarificar mediante una enmienda de modificación que los miembros de la reserva estratégica de talento en ciberseguridad han de ser reservistas, no solo tener consideración de tales. En consecuencia, habrían de recibir igual formación militar y seguir el mismo régimen que el resto de los reservistas. Así se aseguraría su debida integración moral y militar en el seno de las Fuerzas Armadas.*
>
> *Dicho esto, debemos advertir de que, para ampliar sus capacidades, hoy limitadas en exceso, el mando de ciberdefensa no solo necesita una ampliación de sus efectivos, sino también mejorar la preparación de estos, así como la actualización continua de sus medios materiales, equipos y software, y un estudio continuo de investigación y desarrollo. Pero, sin recursos económicos, poco puede hacerse, y*

en un escenario financiero como el que padece la defensa, la ciberdefensa pasa desapercibida.

En cuanto a la enmienda del Grupo Parlamentario Socialista, su oposición a tal propuesta se centró en confiar en los organismos actualmente competentes en materia de ciberseguridad: "Nosotros lo que vemos es: confiar en el Mando Conjunto del Ciberespacio del Ministerio de Defensa; confiar en el Consejo de Seguridad Nacional; confiar en el Centro Criptológico Nacional, CCN, adscrito al CNI como CERT Gubernamental Nacional; confiar en el Incibe, Instituto Nacional de Ciberseguridad de España, y en el CNPIC, Centro Nacional de Protección de Infraestructuras y Ciberseguridad, del Ministerio del Interior", y encomendar al Ministerio de Defensa que estudie primero la cuestión, no predeterminar el modelo y llegar a un estudio realizado en la línea de lo que se ha planteado.

Por parte de Ciudadanos, también alabaron la propuesta, si bien destacaron una serie de matices que les llevaron a discrepar del modelo propuesto en la citada iniciativa legislativa, como son:

El voluntariado, esta especie de ejército de cibervoluntarios que ustedes quieren montar, no es la manera adecuada de enfocar este problema. No digo que no pueda ser un complemento, y yo creo que eso es lo que tiene que resolver el Gobierno, por eso no vamos a votarles en contra de esta Proposición no de Ley, pero sí que instamos al Gobierno a que lo antes posible, como también ha mencionado la portavoz del Grupo Socialista, nos ofrezca una solución, porque yo creo que el Gobierno tiene que dar una solución a esto.

Por último, el representante de Unidas-Podemos también coincide en la necesidad de impulso de una iniciativa como esta, si bien propone hacerlo con cautelas y tras un análisis más profundo de las vías que deben usarse para lograrlo. En este sentido, afirma que:

En ese sentido, nuestro grupo va a hacer un llamamiento a los otros grupos para que intenten acordar y para que esta iniciativa ni se frustre ni tampoco se lleve adelante sin las debidas cautelas.

Con posterioridad, en la sesión del Congreso de 26 de julio de 2021, la Mesa del Congreso de los Diputados admitió a trámite trasladar al Gobierno la Proposición de Ley para la Transformación Digital de España[24].

En la redacción de dicha Proposición de Ley se incluye, en su artículo 60, la creación de un cuerpo de reservistas especializados en tareas de ciberseguridad, bajo el título "reserva estratégica en ciberseguridad" dependiente del Ministerio de Defensa, donde se recogen las finalidades, condiciones, plazos y derechos para poder formar parte de dicho cuerpo. A modo de ejemplo, se reproducen los puntos más relevantes de dicho artículo:

[24] Boletín Oficial de las Cortes Generales (2021, 26 de junio). *Proposición de Ley para la transformación digital de España*:
https://www.congreso.es/public_oficiales/L14/CONG/BOCG/B/BOCG-14-B-173-1.PDF

> 2. Serán reservistas voluntarios pertenecientes a la Reserva Estratégica de Talento en Ciberseguridad los españoles que, en aplicación del derecho y deber constitucionales de defender a España y, habiendo solicitado participar en la correspondiente convocatoria, resulten seleccionados para desempeñar las funciones que se les encomienden bajo la dirección de las autoridades competentes del Ministerio de Defensa, para los cometidos específicos de carácter civil o militar que se señalen. Estos ciudadanos se vincularán de forma temporal y voluntaria con las Fuerzas Armadas por medio de un compromiso de disponibilidad.
>
> 3. Para formar parte de esta reserva específica, el Estado Mayor de la Defensa (EMAD) mediante el Mando Conjunto de Ciberdefensa (MCCD) seleccionará a aquellas personas que, por su experiencia y conocimientos técnicos o de otra índole en la materia, puedan aportar talento a las capacidades existentes en las Fuerzas Armadas. La Reserva Estratégica de Talento en Ciberseguridad, dependerá orgánicamente del EMAD a través del MCCD.
>
> […]
>
> 7. Los reservistas voluntarios cibernéticos pasarán a desarrollar sus funciones al servicio de las Fuerzas Armadas cuando sean activados. No obstante, y por las especiales características de su actividad, estarán en situación de disponibilidad durante todo el período que dure su compromiso. Ello supone que, cuando sea necesario, les podrán ser encomendados cometidos de apoyo a las tareas de ciberseguridad sin necesidad de su incorporación a su unidad de activación en caso de que las circunstancias que concurran así lo hagan necesario.
>
> 8. Los periodos de desarrollo de funciones militares por parte de los reservistas tendrán la consideración de permisos retribuidos, previo acuerdo con la empresa.

Como puede observarse, la propuesta de ciberreserva planteada en España, además de previa es distinta en su enfoque a la propuesta recogida en el Reglamento de Cibersolidaridad, aunque puede considerarse complementaria. Especialmente tras las declaraciones políticas a las que nos hemos referido en los primeros párrafos, donde dejan entrever la necesidad de que la población civil reciba formación en ciberdefensa, pero también que se involucren activamente en acciones de protección de personas e infraestructuras. Con respecto a esto último, la propuesta española permitiría a personas que no desarrollen su actividad en empresas que presten servicios de seguridad gestionada, a que colaboren también en determinadas actividades que puedan hacer más eficaces los esquemas de defensa cibernética del país en determinados momentos.

Más recientemente, en marzo de 2024, el Partido Popular presentaba ante la Comisión de Defensa del Congreso una nueva Proposición no de Ley, esta vez bajo el título “relativa a la creación y regulación de la Reserva Estratégica de Talento en Ciberseguridad dependiente del Ministerio de Defensa para evitar los ciberataques a las instituciones en situaciones de crisis”. Y lo justificaba afirmando que, en este momento, existe una necesidad urgente de contar con una reserva estratégica en materia de ciberdefensa para combatir las amenazas exteriores a nuestro país y a cualquier miembro de la Unión Europea, de la que formamos parte.

En este sentido, si bien esta iniciativa lleva tiempo siendo considerada como una opción idónea para reforzar las capacidades defensivas de España, no es menos ciertos que, desde el ámbito político, existen posturas encontradas donde determinados partidos optan por promover una figura de esta naturaleza, entendiéndola como complemento de los recursos actualmente existentes; mientras que el Gobierno actual considera que España ya dispone de recursos suficientes para abordar los retos de la ciberseguridad, y que no sería necesario dotarnos de un cuerpo de ciberreservistas.

6.1. CONCEPTO.

La ciberreserva puede definirse como una fuerza complementaria, compuesta por profesionales voluntarios del ámbito civil, académico o del sector público, capacitados, para colaborar en la protección contra amenazas cibernéticas en situaciones de crisis o emergencia.

La propuesta de ciberreserva planteada por España es un concepto similar al de las reservas militares tradicionales, no centrada en conflictos armados, sino en la defensa contra ciberataques que, por su gravedad e impacto, alcanzan un nivel suficientemente grave como para considerarse como amenaza para la seguridad nacional, en línea con el espíritu del Reglamento europeo de cibersolidaridad antes citado.

Las personas que la compongan deben poseer capacidades y conocimientos técnicos especializados, así como habilidades de gestión avanzadas en el ámbito de la ciberseguridad. En definitiva, se trata de complementar los recursos disponibles por el Estado afectado en cada momento, destinados a la protección de las infraestructuras más críticas del país.

6.2. COMPONENTES.

Los voluntarios de la ciberreserva son ciudadanos que, en su mayoría, desarrollan su actividad laboral en otras áreas profesionales (derecho, económicas, sociología, antropología, comunicación, etc.) ajenas al ejército o a las fuerzas y cuerpos de seguridad del Estado, que están dispuestos a poner a disposición de su país sus habilidades y conocimientos relacionados con la ciberseguridad en momentos de necesidad.

Su participación puede ser temporal, y pueden ser convocados para responder a incidentes cibernéticos específicos o participar en ejercicios de entrenamiento para mantener un alto nivel de preparación.

6.3. OBJETIVO.

La ciberreserva tiene como objetivo fortalecer las capacidades de ciberseguridad del país, así como proporcionar una respuesta rápida y efectiva ante incidentes cibernéticos, en particular cuando estos afectan a las infraestructuras críticas.

Su creación y mantenimiento debe formar parte de la estrategia de ciberseguridad de una nación, pues su existencia contribuye a la resiliencia de las empresas y, por ende, a la economía en general, y a la seguridad cibernética en todos sus aspectos.

La ciberreserva debe operar de forma coordinada con otras entidades gubernamentales con competencias específicas en ciberseguridad y defensa nacional, como agencias de ciberseguridad, fuerzas armadas, fuerzas de seguridad y centros de respuesta (CERT y CSIRT), para garantizar un apoyo adicional durante la respuesta pública a amenazas cibernéticas que requieran de tal cooperación.

7. LA RESERVA COMO PARTE DE LA GOBERNANZA NACIONAL DE LA CIBERSEGURIDAD.

La reserva de ciberseguridad planteada en el Reglamento de Cibersolidaridad deberá formar parte del modelo de gobernanza de la ciberseguridad nacional, como instrumento que deberá colaborar y coordinarse con el resto de fuerzas de seguridad del Estado para mantener una capacidad de respuesta ante incidentes cibernéticos.

A efectos de su dependencia y de la responsabilidad de su constitución y desarrollo, existen varias opciones, a valorar en cada caso, y sin perjuicio de la intervención de ENISA en el proyecto de reserva europeo soportado por el Reglamento de cibersolidaridad.

En España, los organismos más adecuados para la adopción de un cuerpo de esta naturaleza podrían ser:

a. Ministerio de Defensa: Su participación implicaría una planificación estratégica eficaz y la coordinación de la ciberreserva con otras fuerzas armadas, garantizando que se integre adecuadamente en la estrategia general de seguridad nacional.

b. INCIBE: esta entidad a menudo lidera y coordina los esfuerzos en materia de ciberseguridad vinculados al sector privado (pe., proyecto cibercooperantes[25]) y pueden tener un papel importante en la creación y operación de la ciberreserva. Estas agencias se centran en la detección y prevención de amenazas cibernéticas, así como en la colaboración con otras entidades para garantizar la protección de infraestructuras críticas y sistemas gubernamentales.

c. Ministerio del Interior y cuerpos policiales: Las fuerzas y cuerpos de seguridad, tanto nacionales como autonómicos, pueden desempeñar un papel crucial en la ciberreserva, especialmente en la identificación y persecución de ciberdelincuentes. Trabajan en estrecha colaboración con otras dependencias para llevar a cabo investigaciones y aplicar la ley en casos de delitos cibernéticos.

d. Centros de Reacción ante Ciberataques (CERT/CSIRT): La ciberreserva puede estar vinculada a estos centros, colaborando en la detección temprana de incidentes y en la coordinación de la respuesta.

e. Ministerio de Transformación digital: En algunos países, el Ministerio de TIC o entidad equivalente puede tener un papel relevante en la ciberreserva. Su participación se centra en garantizar la protección y seguridad de las infraestructuras de tecnologías de la información y comunicaciones, que son fundamentales para el funcionamiento del país,

[25] https://www.incibe.es/incibe/cibercooperantes

aunque desde una óptica alejada de lo militar y más cercana al voluntariado civil, lo que permite que sea más flexible en su gestión.

f. Entidades del sector privado: El sector privado también debe estar involucrado en la ciberreserva, especialmente cuando se reclutan reservistas con habilidades y conocimientos especializados en ciberseguridad. La colaboración con el sector privado puede proporcionar una amplia gama de talento y experiencia, pero sin penalizar los intereses de las entidades privadas que sufragan los costes de estos profesionales.

A la vista de estas opciones, correspondería al Gobierno diseñar la estrategia que mejor considere para incorporar la ciberreserva dentro de la estructura del marco de gobernanza actual de la ciberseguridad, teniendo en cuenta que la dependencia directa de entidades públicas (como, por ejemplo, el ejército o los cuerpos policiales) dotan a la ciberreserva de un carácter más rígido y oficial que si, por ejemplo, se vincula a organismos como el INCIBE o al Ministerio responsable de las competencias en materia digital.

8. INTEGRACIÓN DE LA CIBERRESERVA EN LAS ESTRUCTURAS DE SEGURIDAD NACIONAL.

La integración de una futura ciberreserva en las estructuras de seguridad nacional implica la colaboración con diversas dependencias gubernamentales y la sincronización de esfuerzos para garantizar una respuesta coordinada y coherente frente a incidentes cibernéticos.

El proceso para lograr tal integración o, por lo menos, una coordinación aceptable, exige desarrollar una serie de actuaciones, especialmente a nivel público, que adapten el actual escenario normativo y de gobierno de la ciberseguridad al desarrollo eficaz de un cuerpo de tal naturaleza.

Con carácter previo, se debe desarrollar una planificación estratégica que defina los objetivos a largo plazo de una ciberreserva y cómo se alinean con la estrategia de ciberseguridad nacional. Esta planificación debe considerar las capacidades requeridas, las áreas de necesidad y las prioridades de la reserva de ciberseguridad en el contexto de las amenazas emergentes.

Una vez definida esta estrategia, una de las principales actuaciones que deberán plantearse es la que tiene que ver con la adaptación del marco legal y político actual, en el sentido de que permita una definición clara del propósito, responsabilidades, funciones y autoridad de un cuerpo de ciberreservistas compuesto por personal civil. Una iniciativa de tal naturaleza implica la promulgación de normativa específica donde se establezcan las bases para la creación y operación de la ciberreserva, así como su colaboración con otras entidades gubernamentales.

A nivel operativo, la integración de la ciberreserva requiere un entrenamiento y capacitación adecuados para sus reservistas. Esto puede incluir programas de formación en ciberseguridad, ejercicios de simulación de incidentes y entrenamiento en el uso de herramientas y tecnologías relevantes. La capacitación constante mantiene a los reservistas actualizados y preparados para responder a las amenazas cibernéticas.

En cuanto al proceso de activación y despliegue de dicho refuerzo, esto requiere establecer procesos claros y ágiles para la activación y despliegue de la ciberreserva en situaciones de emergencia. Estos procesos deben especificar cómo las personas que la integran son convocadas, cómo se comunican y cómo se coordinan sus acciones con otras entidades involucradas.

Adicionalmente, no hay que olvidar que la integración exitosa de la ciberreserva también implica la colaboración con el sector privado. Esto puede requerir acuerdos de cooperación y compartir mejores prácticas de ciberseguridad con empresas y organizaciones que operan infraestructuras críticas.

Asimismo, es importante evaluar periódicamente la efectividad de la ciberreserva y realizar ajustes y mejoras en función de las lecciones aprendidas y las nuevas amenazas. La retroalimentación constante permitirá optimizar sus capacidades y asegurar una respuesta efectiva a los desafíos cambiantes del ciberespacio.

En resumen, la integración de la ciberreserva en las estructuras de seguridad nacional es un proceso complejo que requiere una planificación estratégica cuidadosa, coordinación con diversas dependencias gubernamentales y el sector privado, y una capacitación adecuada de los reservistas. Con el marco legal y político adecuado, una ciberreserva bien integrada puede ser una herramienta valiosa para fortalecer la ciberseguridad del país y protegerlo contra amenazas cibernéticas en la era digital que, con la llegada de la inteligencia artificial y, próximamente, de tecnologías cuánticas, han diseñado un escenario más complejo y sofisticado que sigue dificultando la gestión eficaz de ciberincidentes.

9. EL PERFIL DEL CIBERRESERVISTA: HABILIDADES Y COMPETENCIAS.

Las habilidades requeridas a los ciberreservistas son fundamentales para garantizar que puedan enfrentarse con éxito a los desafíos que plantean las situaciones de crisis nacional. Estas capacidades deben ser diversas y actualizadas para adaptarse a la evolución constante de las tecnologías y de las tácticas cibernéticas. Sin perjuicio de los distintos perfiles de ciberreservista que puedan definirse, algunas de las habilidades clave que deben poseer sus integrantes incluyen:

1. Conocimientos en ciberseguridad: Los ciberreservistas deben tener un sólido conocimiento en ciberseguridad, comprendiendo los principios fundamentales de la seguridad informática, la protección de redes, sistemas y aplicaciones, así como las metodologías de *hacking* ético para comprender cómo piensan y actúan los atacantes.

2. Análisis de amenazas: Es esencial que los ciberreservistas sean capaces de analizar y comprender las amenazas cibernéticas emergentes. Deben ser capaces de identificar patrones de ataque, reconocer técnicas maliciosas y determinar la gravedad y el alcance de los incidentes para responder adecuadamente. Estas habilidades permitirían mejoras las capacidades analíticas y de inteligencia actuales.

3. Respuesta a incidentes: Los ciberreservistas deben estar capacitados en la gestión y respuesta a incidentes cibernéticos. Esto incluye la habilidad de detectar intrusiones, contener y mitigar ataques en curso, y llevar a cabo investigaciones forenses

para determinar el origen y la naturaleza de un incidente. La aportación de los ciberreservistas en este campo mejoraría las capacidades de identificación y gestión de eventuales incidentes, reforzando las capacidades técnicas de reacción y mitigación.

4. Programación y desarrollo seguro: Un conocimiento sólido de lenguajes de programación y desarrollo seguro es esencial para identificar y corregir vulnerabilidades en el *software* y aplicaciones utilizadas en el país. Esto puede implicar el desarrollo de parches o soluciones para mitigar riesgos de seguridad.

5. Ciberinteligencia: Los ciberreservistas deben ser capaces de recopilar y analizar inteligencia cibernética para anticipar y contrarrestar posibles amenazas. Esto implica el seguimiento de actores maliciosos, su infraestructura y tácticas, y la colaboración con otras agencias para compartir información relevante. Este refuerzo mejoraría las capacidades preventivas de España, así como incrementaría el conocimiento de los ataques, los agentes responsables, sus motivaciones y, por ende, esta información permitiría a las empresas y organismos españoles a incrementar su capacidad de resiliencia.

6. Comunicación efectiva: La comunicación efectiva es fundamental para coordinar esfuerzos con otras entidades gubernamentales, compartir información relevante y explicar conceptos técnicos de manera comprensible para los no expertos, especialmente los ciudadanos y empresarios.

7. Pensamiento crítico y resolución de problemas: Los ciberreservistas deben ser pensadores críticos y hábiles en la resolución de problemas. Deben poder enfrentar situaciones complejas y desconocidas, tomar decisiones rápidas y efectivas, y adaptarse a escenarios cambiantes. Esto puede permitir incorporar nuevas visiones, perspectivas y modos de gestionar las amenazas, aportando un valor añadido a los equipos actuales.

8. Conocimiento profundo del entorno normativo y regulatorio. Esto, al igual que en resto de apartados, fomentaría la captación y el desarrollo de talento en estas materias, así como la formación y mejora del entorno regulatorio, cada vez más complejo y necesario.

9. Trabajo en equipo y colaboración: La ciberseguridad es un esfuerzo colaborativo que requiere la capacidad de trabajar en equipo con otros especialistas en ciberseguridad, fuerzas de seguridad y agencias gubernamentales para abordar desafíos cibernéticos de manera coordinada y efectiva. Gracias a ello, podría fomentarse la cohesión territorial, que es uno de los objetivos que ya se recogen, por ejemplo, en la antigua Estrategia Nacional de Inteligencia Artificial.

10. Ética y responsabilidad: Los ciberreservistas deben adherirse a altos estándares éticos y responsabilidad en el manejo de la información y la realización de sus tareas. La confidencialidad, la integridad y la responsabilidad son fundamentales en la ciberseguridad.

En resumen, los ciberreservistas deben poseer un conjunto diverso de habilidades técnicas y de otra naturaleza para enfrentar los desafíos de la ciberseguridad en la actualidad. Su conocimiento en ciberseguridad, análisis de amenazas, respuesta a incidentes y colaboración efectiva son esenciales para asegurar una respuesta rápida y

efectiva ante incidentes cibernéticos y proteger la seguridad y resiliencia del país en el ciberespacio.

10. POLÍTICAS Y LEYES RELACIONADAS CON LA CIBERRESERVA.

La implementación efectiva de una ciberreserva, especialmente en el caso que tiene que ver con la propuesta española de crear un cuerpo de voluntarios civiles, requiere de un marco normativo y legal sólido que establezca las reglas y responsabilidades para su operación. Estas políticas y leyes deben estar diseñadas para garantizar que la ciberreserva funcione de manera coordinada, eficiente y con pleno respeto a las normas legales y éticas.

A continuación, se detallan algunos aspectos clave relacionados con la regulación de la ciberreserva:

a. Legislación de creación: los países que han establecido una ciberreserva (pe., el caso de Francia) generalmente cuentan con leyes o decretos específicos que autorizan y definen su creación. Estas legislaciones pueden establecer la misión y el propósito de la ciberreserva, así como los mecanismos para su reclutamiento, entrenamiento y activación en caso de crisis.

b. Autoridad y coordinación: las políticas y leyes deben especificar la autoridad que tiene la ciberreserva y cómo se coordinará con otras entidades, como las fuerzas armadas, agencias de inteligencia, organismos de ciberseguridad y el sector privado. Es importante establecer la estructura de mando y control para garantizar una respuesta coherente y sin fisuras en caso de un incidente cibernético.

c. Protección de datos y privacidad: las actividades de la ciberreserva a menudo implican el acceso a información sensible y datos críticos. Por lo tanto, es vital que las políticas y leyes establezcan salvaguardias para proteger la privacidad y la confidencialidad de la información a la que acceden los reservistas cibernéticos durante sus operaciones.

d. Uso de habilidades civiles y sector privado: algunas ciberreservas incorporan expertos del sector privado que tienen habilidades especializadas en ciberseguridad. Las políticas y leyes nacionales aplicables deben abordar cómo se puede integrar a estos reservistas y cómo se manejarán posibles conflictos de intereses con sus empleadores privados.

e. Responsabilidades y deberes: las políticas y leyes deben establecer las responsabilidades y deberes de los reservistas cibernéticos. Esto puede incluir la obligación de mantener sus habilidades actualizadas, participar en ejercicios de entrenamiento y responder de manera efectiva ante incidentes cibernéticos.

f. Coordinación internacional: en un mundo altamente interconectado, la ciberreserva abordará desafíos transnacionales. Las políticas y leyes deben considerar la cooperación y coordinación internacional con otras ciberreservas o entidades similares en otros países para abordar amenazas cibernéticas extraterritoriales.

g. Rendición de cuentas y evaluación: la regulación deberá establecer mecanismos para evaluar la eficacia de la ciberreserva y garantizar su rendición de cuentas. Esto puede incluir auditorías periódicas, informes de actividades y revisiones para mejorar continuamente las capacidades de respuesta.

En general, las políticas y leyes relacionadas con la ciberreserva son fundamentales para crear una base sólida para su funcionamiento, garantizar su efectividad y proteger los intereses nacionales en el ciberespacio. Estas políticas deben adaptarse a las cambiantes amenazas y desafíos cibernéticos para asegurar que la ciberreserva siga siendo relevante y capaz de proteger los activos digitales y la infraestructura crítica del país.

11. EJEMPLOS DE PAÍSES QUE DISPONEN DE UNA CIBERRESERVA.

1. Estados Unidos[26].

Los Estados Unidos cuentan con la conocida como "*U.S. Cyber Reserve*". Esta entidad está compuesta por expertos en ciberseguridad de diferentes sectores, incluyendo el gobierno, la industria privada y el sector académico.

Los miembros de la reserva están capacitados para responder a incidentes cibernéticos y proporcionar apoyo en caso de emergencias relacionadas con la ciberseguridad.

2. Reino Unido[27].

El Reino Unido estableció su "*UK Cyber Reserve*" para abordar la creciente amenaza de los ciberataques. Esta ciberreserva está formada por especialistas en ciberseguridad reclutados del sector privado y de las fuerzas armadas.

Trabajan junto con el Centro Nacional de Seguridad Cibernética (NCSC) para proteger las infraestructuras críticas del país y garantizar la ciberseguridad nacional.

3. Estonia - "*Estonian Defense League's Cyber Unit*"[28].

Estonia, un país conocido por su enfoque avanzado en la ciberseguridad, ha desarrollado una unidad cibernética dentro de la Liga de Defensa de Estonia (*Kaitseliit*).

Esta unidad tiene como objetivo proporcionar una capacidad adicional para defenderse contra ciberataques y contribuir a la resiliencia cibernética del país.

[26] Brumfield, Cynthia (2024, 24 de abril). *Civilian cyber reserves gaining steam at the US federal and state levels.* https://www.csoonline.com/article/1297690/civilian-cyber-reserves-gaining-steam-at-the-us-federal-and-state-levels.html

[27] Gobierno del Reino Unido (2024, junio). *Joint Cyber Reserve Force.* https://www.gov.uk/government/groups/joint-cyber-reserve-force

[28] Ministerio de Defensa de la República de Estonia (2024, junio). *Cyber Command.* https://mil.ee/en/landforces/cyber-command/

4. Singapur[29].

Singapur ha creado el Grupo de Defensa Cibernética de las Fuerzas Armadas de Singapur (Singapore Armed Forces Cyber Defense Group) para abordar las amenazas cibernéticas y garantizar la seguridad de sus sistemas de información. El grupo está compuesto por reservistas altamente calificados con experiencia en ciberseguridad.

5. Israel - "*Israel Defense Forces Cyber Unit*"[30].

Israel es conocido por su capacidad en ciberseguridad y ha establecido una unidad cibernética dentro de las Fuerzas de Defensa de Israel (IDF). La unidad se centra en la defensa cibernética, la inteligencia y la lucha contra las amenazas cibernéticas que enfrenta el país.

Israel adapta su enfoque y estructura de ciberreserva según sus necesidades específicas y la naturaleza de las amenazas cibernéticas a las que se enfrenta.

6. Francia – "*Réserve Citoyenne Cyberdéfense*"[31].

La ciberreserva en Francia, conocida como "Reserva Ciudadana de Ciberdefensa", es un programa lanzado por el gobierno francés para movilizar a expertos civiles en ciberseguridad y tecnologías de la información para reforzar la defensa cibernética del país. Este programa se enmarca dentro de los esfuerzos más amplios de Francia para protegerse contra las amenazas cibernéticas y fortalecer su ciberresiliencia.

La Reserva Ciudadana de Ciberdefensa fue creada en 2014, y está abierta a ciudadanos franceses que posean habilidades y experiencia en áreas relacionadas con la ciberseguridad, como la seguridad de la información, el análisis forense digital, la gestión de incidentes, y la protección de redes y sistemas, entre otros. El objetivo principal de esta iniciativa es proporcionar un recurso adicional y complementario a las capacidades de defensa cibernética del gobierno y las fuerzas armadas.

Los reservistas de ciberdefensa participan en actividades como la detección y respuesta a incidentes cibernéticos, la evaluación de vulnerabilidades en sistemas informáticos, la concienciación y educación en ciberseguridad, y la investigación y desarrollo en tecnologías de seguridad. También pueden ser movilizados en caso de crisis cibernéticas o ataques cibernéticos de gran escala para apoyar los esfuerzos de defensa y respuesta del gobierno.

España podría obtener un valioso conocimiento de la experiencia de tales países, y reforzar el intercambio de información y diseñar intercambios de profesionales que les permita aumentar su nivel de formación y conocimientos en materia de ciberseguridad y, en particular, de prevención y gestión de ciberataques.

---

[29] Mnisterio de Defensa de Singapur (2024, junio): https://www.mindef.gov.sg/web/portal/mindef/home

[30] Ministerio de Defensa de Israel (2024, junio). *C4i and Ciber Defense directorate.* https://www.idf.il/en/mini-sites/directorates/c4i-and-cyber-defense-directorate/c4i-and-cyber-defense-directorate/

[31] Ministerio de Defensa de la República francesa (2024, junio). *La réserve.* https://www.defense.gouv.fr/comcyber/nous-rejoindre/reserve

12. CONCLUSIONES.

Con el Reglamento de Cibersolidaridad se creará una reserva europea de ciberseguridad que dote de recursos a la Unión Europea, a los efectos de mejorar sus capacidades de defensa cibernética frente a incidentes de alto impacto. Esto supone una oportunidad para España a la hora de formar y atraer talento en un sector cada vez más necesitado de profesionales cualificados.

Esta nueva línea de ciberdefensa, denominada cyber shield, se estructurará a través de una red de SOC públicos y de proveedores privados de servicios de seguridad gestionada, que aportarán profesionales de alta capacitación y conocimientos técnicos en materia de ciberseguridad para hacer frente a aquellas amenazas que excedan de las capacidades normales de defensa.

Sin perjuicio de tal iniciativa, y complementariamente a aquella, algunos países han diseñado un cuerpo de ciberreservistas, compuesto por personal civil con experiencia en la gestión de incidentes de ciberseguridad en el mundo de la empresa y de la universidad, que puedan aportar su conocimiento y experiencia para ayudar a complementar las capacidades de los servicios públicos competentes en esta materia, con el objetivo de mejorar la resiliencia nacional ante unas amenazas cibernéticas cada vez mayores y más sofisticadas.

En este caso, para poder cubrir las nuevas necesidades de sensibilización, concienciación y capacitación de la población civil en la defensa de las redes y sistemas públicos y privados, así como la información que se almacena en ellos, los activos digitales y las infraestructuras en general, exige diseñar e implementar un cuerpo de reservistas voluntarios expertos en la materia, que puedan prestar apoyo puntual y extraordinario en determinados momentos.

Al objeto de diseñar un cuerpo de esta naturaleza, España tiene sobrada experiencia en la organización de un cuerpo de reservistas, por lo que el diseño de un cuerpo de ciberreservistas puede plantearse de forma adicional y complementaria a las actuales capacidades de la reserva de ciberseguridad nacional, además de coordinada con el resto de cuerpos de ciberreserva de otros países, todos ellos referentes en el ámbito de la ciberseguridad y que han sabido aprovechar esta iniciativa para desarrollar una industria robusta en esta materia, así como un posicionamiento geoestratégico destacado en este ámbito de la seguridad nacional.