Francisco Pérez Bes
Digital Law Partner at Ecix Tech
PhD student in Public Law from
the University of Salamanca
Professor of Cybersecurity Law
Francisco de Vitoria University (UFV)

THE REGULATION OF A CYBERSECURITY RESERVE. A VIEW FROM THE EUROPEAN CYBERSOLIDARITY REGULATION

THE REGULATION OF A CYBERSECURITY RESERVE. A VIEW FROM THE EUROPEAN CYBERSOLIDARITY REGULATION

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.

ABBREVIATIONS

Art.: Article

BOCG: Official Gazette of the Spanish Parliament

BOE: Official State Gazette

CE: European Commission

CERT: Computer Emergency Response Team

CSIRT: Computer Security Incident Reaction Team

OJEU: Official Journal of the European Union

ENISA: European Union Cybersecurity Agency

GC: Guardia Civil

INCIBE: Spain's National Institute for Cybersecurity

NLP: Non-Legislative Proposal

SOC: Security Operations Centre

EU: European Union

1. INTRODUCTION: A CYBERSECURITY RESERVE FOR CYBERSOLIDARITY.

On 22 March 2024, the Spanish press published an article entitled "EU asks citizens to prepare to face *all dangers*", an article that discussed the military threat facing European citizens in a short period of time (there is talk of an armed conflict with Russia by 2026). Furthermore, it was stated that "war goes beyond launching missiles and society must be aware", warning about this in a clear change of language. Talk of civil society preparedness marks a change of pattern in the EU. The article adds a series of data with a direct impact on continental cybersecurity, warning that "the EU, aware of its vulnerability, fears cyber-attacks that paralyse services, attacks on civilian infrastructure such as energy installations and telecommunications cables, and massive disinformation campaigns"[1].

A few days earlier, the Spanish Defence Minister, Margarita Robles, was interviewed by the same media, where she responded to the question of whether the threat of war could be considered real, given the call by several European leaders for the rearmament of the European Union. In that interview, she stressed that "the threat is total and absolute. [...] Europe must be aware that the danger is very close; it is not just a hypothesis, it is real. The countries bordering Russia are well aware of this; perhaps those of us in the south do not share that perception, but civilisation can be attacked by unscrupulous people like Putin"[2].

Just over a year earlier, on 10 November 2022, the Joint Communication on a European Cyber Defence Policy announced an initiative on cyber-solidarity[3], which identified a number of objectives. These included the creation of specific European cyber defence capabilities to deal with cybersecurity incidents considered significant due to their high level of severity.

The aforementioned document already envisaged that such resources should be built on strengthening cyberattack detection and response capabilities, promoting a European infrastructure of Security Operations Centres (commonly known as SOCs) that should gradually support the building of a European-wide cybersecurity standby corps of private managed security providers. These providers will be designated as such on the basis of their level of reliability and should aim primarily to strengthen the security of critical infrastructures against high-impact cyber incidents.

Recently, in March 2024, in line with the deadlines of the aforementioned initiative, the European Union (EU) adopted the *Cybersolidarity Act* as part of its cybersecurity legislative package: a Regulation on cybersolidarity that aims to strengthen the Union's capabilities to detect, prepare for and respond to significant and large-scale

---

[1] El País newspaper (2024, March). *The EU calls on society to prepare for the full range of dangers and a changing threat landscape.*
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, March). *The threat of a Russian attack is absolute*.
https://www.rtve.es/play/videos/fin-de-semana-24h/robles-amenaza-ataque-rusia-absoluta/16019094/

[3] European Commission (2022, 10 November). *Cyber defence: EU boosts measures against cyber threats* [press release].
https://ec.europa.eu/commission/presscorner/detail/es/ip_22_6642

cybersecurity threats and attacks[4]. These capabilities may also be required by third countries affected by large-scale cyber-incidents, if they have a cooperation agreement with the European Union for this purpose[5].

One of the measures envisaged in this new regulation is the creation of a cybersecurity pool which, according to the European Commission itself, "will consist of incident response services from private service providers ("trusted providers"), which can be deployed at the request of Member States or Union institutions, bodies and agencies to help them deal with significant or large-scale cybersecurity incidents"[6].

In other words, the Act provides for the creation of a European cyber reserve of cyber incident prevention and response services provided by trusted providers, selected in accordance with the criteria set out in the Regulation. Potential users of the services of the Reserve include Member States' cyber crisis management authorities and CSIRTs, as well as the Union institutions, bodies, offices and other bodies.

In addition, the document considers that the European Commission should be responsible for establishing the EU Cybersecurity Reserve, and may entrust all or part of its funding, operation and management to the European Cybersecurity Agency (ENISA)[7].

In this sense, Recital 33 of the initial proposal for a Regulation reflected the advisability of having a cybersecurity reserve, with the ultimate aim of creating a European cyber shield to reinforce the security of the strategic infrastructures of the Member States and, therefore, those of the European Union as a whole[8]:

> *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 the 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*

[4] Vid. Art. 1.1 of the Proposal for a Regulation: "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] European Commission (2024, March). *The EU Cyber Solidarity Act*. 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] Free translation: The services of the EU Cybersecurity Reserve should support national authorities in providing assistance to affected entities operating in critical or highly critical sectors as a complement to their own actions at the 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 considered when assessing the Member State's request. The services of the EU Cybersecurity Reserve can also be used to support EU institutions, bodies and agencies under similar conditions.

services from the EU Cybersecurity Reserve may also serve to support Union institutions, bodies and agencies, under similar conditions.

More specifically, Chapter II, Article 3, paragraph one of the proposal for a Regulation, entitled "the European Cyber Shield", refers to the establishment of this figure with the following wording:

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').

If we look at the articles of the aforementioned *Cybersolidarity Act,* it is articles 12 and following that regulate the constitution, operation and requirements to be met by the providers that constitute the cybersecurity reserve in the sense described above.

Finally, it should be borne in mind that the approval and subsequent entry into force of this new cybersolidarity regulation will entail the modification of certain European regulations such as, for example, the Digital Europe Programme[9].

As an example of some of the changes proposed in the above-mentioned regulation, the following text is proposed to be included in the current Article 6 of Regulation 2021/694:

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

Finally, we must distinguish this initiative from some others, also at this level of international collaboration. Thus, for example, we find the one presented in 2023 by former Spanish senator José Cepeda, who was commissioned by the Inter-Parliamentary Union (IPU) to draft a report on cybercrime, cyberattacks and cybercrime, new threats to global security. In this work, the creation of a new corps of "cyber blue helmets" was proposed to protect, through the UN, citizens from cyber-terrorism and cybercrime. In

[9] Regulation 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240
https://www.boe.es/buscar/doc.php?id=DOUE-L-2021-80609

turn, the European Union continues to carry out actions focused on cybersecurity and the fight against cybercrime[10].

According to [11], this proposal has gained unanimous support and global recognition, although it is hoped that progress towards its consolidation can be made at the next global summit, scheduled for 2024.

2. FUNCTIONS OF A CYBER RESERVE IN THE DIGITAL AGE.

In today's increasingly hyperconnected digital society, the approach to creating a support body external to the public's own structures and resources has traditionally been based on the spirit of public-private collaboration, focused on the technical resolution of cybersecurity incidents.

One of the main functions of this qualified support, focused on eminently technical aspects, would be to complement existing public capacities, which - due to budgetary, knowledge or resource constraints - may need additional reinforcement at certain times. And, to this end, it is considered that such support can be effectively provided by the private sector, which presumably has numerous technical, knowledge and experience capabilities, among others. This can assist in the proper management of certain cybersecurity incidents, especially the more complex ones.

To this end, the approach to effective collaboration requires designing a body of professionals with a high degree of flexibility and professional experience to actively support the management of specific incidents and emergency situations which, due to their severity, might exceed the capacities of the entities concerned or the competent authorities.

This would be the case for Security Operations Centres (SOCs), as set out in the proposed Regulation on cyber solidarity when it foresees that they can request the support of managed security providers in certain cases. But it could also be the case for Cyber Incident Response Teams (CSIRTs), as foreseen in Articles 10 et seq. of the commonly known NIS 2 Directive[12].

As is well known, this Directive reserves the reactive powers to manage cybersecurity incidents of particular relevance, when they affect essential entities or important companies to the CSIRTs.

With regard to CSIRTs, the ninth additional provision of Law 34/2002, on information society services and electronic commerce, already referred to this organisation (still under the traditional name of CERT), as follows:

---

[10] European Council (2024, June). *Cybersecurity: how the EU is combating cyber threats* 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

[12] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures to ensure a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing Directive (EU) 2016/1148

> 1. Information Society service providers, domain name registries and registration agents established in Spain are obliged to cooperate with the competent CERT in the resolution of cybersecurity incidents affecting the Internet network and to act in accordance with the security recommendations indicated or established in the codes of conduct derived from this Law.
>
> Public bodies, agencies or any other public sector entity operating security incident response teams shall cooperate with the competent authorities for the provision of the technical evidence necessary for the prosecution of crimes arising from such cybersecurity incidents.
>
> 2. For the exercise of the above functions and obligations, Information Society service providers, while respecting the secrecy of communications, shall supply the necessary information to the competent CERT, and to the competent authorities, for the appropriate management of cybersecurity incidents, including the IP addresses that may be compromised or involved in them.

At this point, it is necessary to identify the main reasons why it is advisable for European countries to have an additional, complementary and extraordinary intervention force, such as a corps of cyber-reservists, in the sense proposed by the cyber-solidarity regulation:

Firstly, we can highlight the rapid and constant evolution of cyber threats which, from a cybersecurity perspective, require organisations to carry out constant tasks of identification, description and up-to-date knowledge of their functioning and impact.

In light of this, and in the knowledge that cyber threats evolve as technology advances, cyber resilience can adapt quickly and effectively to new threats, technologies and tactics used by attackers.

The functional dependence of critical and strategic infrastructures on technology is also an undeniable fact, particularly in view of the fact that the resilience of such infrastructures and of the operators that support and manage them is essential to ensure the continuity of essential and critical services.

Likewise, a resource such as the cyber reserve makes it possible to structure specialised training for highly qualified professionals committed to national defence, including in areas considered "non-technical" (intelligence, law, economics, communication, etc.) where there is a known lack of resources in public structures.

In this regard, it should not be forgotten that national security, as defined in the National Security Law 36/2015 of 28 September[13], and in the National Security Strategy 2021[14], is not limited to traditional military defence, but also encompasses the protection of the economy, health, the environment and, of course, protection against cyber threats.

[13] Law 36/2015, of 28 September, on National Security.
https://www.boe.es/buscar/act.php?id=BOE-A-2015-10389
[14] Department of Homeland Security (2024, June). *National Security Strategy*
https://www.dsn.gob.es/es/estrategias-publicaciones/estrategias/estrategia-seguridad-nacional-2017

Therefore, in view of these reasons that justify the creation of a cybersecurity reserve at the initiative of the State itself, it is essential to be able to set up a cooperation structure between such a cybersecurity reserve and the private sector (in this case, through managed security services). Indeed, most critical infrastructures and services are in private hands, and there are many people who can - based on their experience - provide useful insights and knowledge to protect networks and systems, while strengthening and improving coordination with the private sector, as already foreseen in the critical infrastructure resilience regulation.

3. ORIGINS OF THE CYBER RESERVE.

The idea of setting up a specialised technical support force dates back to the very beginnings of the Internet, when military and intelligence agencies began to recognise their shortcomings and limitations (in knowledge and resources) in handling certain security incidents, while the private sector had people whose knowledge and skills could be of great help at times when national security could be affected by a high-impact cyber incident of some kind.

We witnessed this with the emergence of *Computer Emergency Response Teams (CERTs*), which arose in response to the need to protect networks and information systems and the information they contained in the face of the first threats that were beginning to appear on the Internet.

Faced with this scenario, the US agency DARPA *(Defence Advanced Research Projects Agency*)[15], funded a project to improve the coordination of responses to new cyber threats, consisting of the design and creation of a network of technical teams specialised in reactively managing cybersecurity incidents, known as *Computer Emergency Reaction Teams* or CERTs.

It is well-known that the nature of cyberthreats has become increasingly complex, diverse and pluralistic, and their targets have expanded to include governments, businesses and citizens. This has led to the need to develop ever broader and more flexible response capabilities to deal with these emerging threats.

One of the important milestones in the evolution of cyber-resilience was the recognition that cyber-attacks can have devastating effects on civilian life and the economy[16], which - as we will see - has led more and more countries to design formal cyber-resilience programmes to protect their populations and national interests.

In this sense, the cyber reserve - as envisaged in the European Regulation - can play an important role in national security by providing a highly trained and adaptable collaborative response force that can be rapidly mobilised to address cyber incidents and

[15] Darpa.mil
[16] Pérez Bes, F. (2022) *Cyberattacks on listed companies and their impact on share value.* Esys Foundation: https://fundacionesys.com/es/los-ciberataques-en-la-empresa-cotizada-y-su-impacto-en-el-valor-de-las-acciones/

protect critical infrastructure or other resources that may be threatened [17]. The cybersecurity reserve, as foreseen in the Cybersolidarity Act, would work closely with the competent authorities to strengthen the defensive capabilities of the affected country and reduce the impact of specific cyber attacks.

4. OBJECTIVES AND FUNCTIONS OF THE CYBER RESERVE.

A well-designed cyber reserve should have a number of key objectives and functions that will guide its role in the national cyber security ecosystem and its contribution to protecting against cyber threats.

Among the aforementioned objectives, as indicated above, the main one is to respond effectively to cyber incidents in circumstances where additional resources are needed to ensure better and more efficient management of a national crisis situation resulting from such an incident.

Furthermore, the cyber reserve is obliged to collaborate with governmental entities, which means that this body must be placed at the service of the public authorities at highly exceptional times, in order to ensure a more efficient response to massive cyberattacks and, consequently, to reinforce the protection of national interests.

Because of this, cybersecurity reservists must be trained to assist in the detection, analysis and mitigation of high-impact cyber-attacks, as required by the aforementioned Cybersolidarity Act, which requires professionals who make up the cybersecurity reserve to have highly specialised technical knowledge.

In this sense, the proposed Regulation seems to suffer from a shortcoming in requiring -only- technical training in the response to cyber-incidents, forgetting the relevance of management skills and knowledge, especially when it comes to collaborating in minimising damage, restoring normality to the affected systems and defending the rights of citizens and the reputation of the affected entity.

This need is an opportunity for European countries to promote such training, both directly from the public authorities (in Spain, for example, with initiatives such as INCIBE's *Summer Bootcamp* [18], the *National Cyberleague* of Guardia Civil [19], or C1b3rw4ll of the National Police[20]), and through programmes designed and carried out by companies that voluntarily wish to collaborate with an initiative such as the cyber reserve.

At this juncture, it is worth remembering that another important objective of the cyber reserve will be to promote cybersecurity awareness among the general public and private companies in particular. In this respect, reservists can play an active role as educators in good cyber security practices (a concept that the NIS2 Directive refers to as

[17] Council of Europe (2023, 20 December). Cybersolidarity Act: Member States agree on a common position to strengthen cybersecurity capabilities in the EU: 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/

[18] https://www.incibe.es/en/events/summer-bootcamp

[19] https://www.nationalcyberleague.es/

[20] https://c1b3rwall.policia.es/

"cyber hygiene"), and in preventing incidents through awareness-raising and sensitisation in their organisations, but also in educational establishments and especially in vulnerable groups, such as children or the elderly.

In view of the above, it can be concluded that a cybersecurity standby system such as the one proposed by the European Cybersolidarity Act (through the SOC network) does not appear to be mutually exclusive with the existence of a corps of specialised cybersecurity professionals, who do not necessarily work for managed security providers, but who, at certain times, may be useful during the process of managing a cybersecurity incident of significant severity.

5. BENEFITS OF HAVING A CYBER RESERVE.

The creation and maintenance of a cyber reserve can bring a number of significant benefits in the area of national cybersecurity and protection against cyber threats related to state resilience.

At the operational level, where responsiveness is key in the detection and management of a high-severity incident, the cyber reserve should be a resource with a high level of availability to act in times of urgency and management capacity. Immediate availability will enable rapid and effective mobilisation to respond to cyber incidents, minimising the impact of attacks and accelerating the recovery of affected systems and services.

In the event of a crisis or a major cyberattack, the cyber reserve provides valuable support to reinforce national security efforts. Their presence can help mitigate the effects of an incident and ensure the continuity of the country's critical operations.

Moreover, it must be a quality resource, complementing the state's existing cybersecurity capabilities. In other words, its specialised focus on cyber threats and expertise in security technologies allow it to address challenges that exceed the usual resources available.

This added value is provided with a high degree of flexibility and adaptability, as the cyber reserve is composed of volunteers from various professional backgrounds, offering a great diversity of skills and knowledge. This diversity makes it possible to adapt to different situations and to address a wide range of cyber threats effectively, not only in the purely technical aspect, but also in other aspects such as legal, economic, sociological, communication, psychological, etc.

In addition, cyber reserve can foster greater public-private collaboration on cybersecurity, as by recruiting private sector specialists, links are established that enable them to share knowledge and best practices, thereby improving security at the business level.

As regards its composition, this initiative offers citizens the opportunity to contribute their skills and knowledge to the protection of the country's national security and critical infrastructure. This citizen participation in cybersecurity issues can also strengthen the sense of ownership and responsibility towards the protection of the nation.

Being part of the cyber reserve also offers reservists the opportunity to develop their technical skills, access advanced training programmes and establish structured connections with other cyber security professionals, both in government and in the private sector.

In short, the cyber reserve stands as a regulatory initiative that can bring significant benefits to national and European cybersecurity, including rapid and effective incident response, cybersecurity capacity building, collaboration with the private sector, citizen participation in national security and professional development of reservists, etc.

These benefits undoubtedly make the cyber reserve a valuable tool for strengthening the country's resilience and protection in cyberspace.

6. THE CYBER RESERVE PROPOSAL IN SPAIN.

In Spain, on 25 March 2020, a Non-Legislative Proposal (PNL) was presented with the aim of setting up a cyber reserve, with the title "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" (Non-Legislative Proposal on the creation and regulation of the Strategic Cybersecurity Talent Reserve under the Ministry of Defence to prevent cyberattacks on institutions in crisis situations). [21].

On 21 April 2021, the Defence Committee agreed to approve the aforementioned proposal, urging the Government to[22]:

> 1. Study the creation of a strategic cybersecurity talent pool, with a civilian and military component, to strengthen the capabilities of the Ministry of Defence in support of its needs in the specific area of cyberdefence, through the selection of individuals whose experience and technical or other expertise would enhance existing capabilities.
>
> 2. Study the possibilities of the secondment model under the fulfilment of the criteria and conditions to be determined, which will enable the talent retained to be shared with private companies. Consider the current system of "Voluntary Reservists" of the Armed Forces as a reference for secondment.
>
> 3. Consider the current system of "Armed Forces Voluntary Reservists" as a reference for secondment.

With regard to this initiative, in the Journal of Congress[23], dated 21 April 2021 (file number 161/000461), the Popular Parliamentary Group in that House (Mr Callejas

[21] Defence Committee of the Congress of Deputies, file number 161/000461.
[22] Official Gazette of the Spanish Parliament (BOCG) of 20 May 2021, number 276: https://www.congreso.es/public_oficiales/L14/CONG/BOCG/D/BOCG-14-D-276.PDF#page=5
[23] Official Gazette of the Spanish Parliament (2021, 21 April). *Journal of Sessions of the Congress of Deputies*. 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&_publicac

Cano) presented a new proposal, in the form of a PNL, regarding the creation and regulation of the strategic cybersecurity talent pool under the Ministry of Defence to prevent cyberattacks on institutions in crisis situations.

Among the arguments put forward for the debate on this proposal, a series of data stand out regarding the current resource situation of the Joint Cyberspace Command, created on 27 July 2020, which has just over two hundred troops and activates some fifteen volunteer reservists per year, it is claimed.

The age of the volunteers is also a relevant element when analysing an efficient and sustainable cyber reserve model. In this respect, the information provided in that parliamentary intervention states that:

> *In the master's degree in Data Science at the Universidad Politécnica de Madrid, the average age of the teaching staff is only thirty-three years old. Currently, the voluntary reserve model in Spain, as it stands, favours experience over talent or knowledge. It is mathematically impossible for any of the profiles that may be requested for cyber defence to achieve the status of voluntary reservist, simply because of the handicap of their youth.*
>
> *The development of cyber defence capabilities requires 80 % talent as opposed to 20 % experience, and it is therefore proposed to modify the model for recruiting volunteer reservists in order to be able to bring in young talent which, in the case of technical profiles, is more plentiful.*

This policy approach concludes that:

> *Cybersecurity must be cross-cutting throughout the Armed Forces, as it is in healthcare. The creation of a specific corps or weapon along the lines of a common corps that applies to all three armies should be explored. While this would be the easiest solution, other options could be the creation of a single cyber defence speciality for the armed forces or actually considering the creation of a fourth army, the cyber army.*

Two amendments were tabled to the initiative described above, one from the VOX parliamentary group and the other from the socialist parliamentary group. Ciudadanos and Podemos also took the floor to give their views on the matter.

With regard to the first (VOX), it was a modification amendment to the PNL, in the sense of complementing its proposal to highlight the need to increase the appropriations allocated to the purpose of the fight against cyberattacks by a cyber reserve, which was done through the following arguments:

> *The voluntary reserve would indeed be an excellent solution. We only wanted to clarify by means of an amending amendment that members of the strategic cybersecurity talent pool should be reservists, not only be considered as such. Consequently, they would have to receive the same military training and follow*

iones_mode=mostrarTextoIntegro&_publicaciones_legislatura=XIV&_publicaciones_id_texto=(DSCD-14-CO-367.CODI.)#(P%C3%A1gina7)

the same regime as other reservists. This would ensure their proper moral and military integration into the Armed Forces.

That said, it should be noted that, in order to expand its capabilities, which are currently too limited, the cyber defence command needs not only to expand its personnel but also to improve their readiness, as well as continuous updating of the material resources, equipment and software, and an ongoing study of research and development. But without financial resources, little can be done, and in a financial scenario like the one experienced by defence, cyber defence goes unnoticed.

As for the Socialist Group's amendment, its opposition to such a proposal focused on relying on the bodies currently competent for cybersecurity: "What we see is: trust in the Joint Cyberspace Command of the Ministry of Defence; trust in the National Security Council; trust in the National Cryptologic Centre, CCN, attached to the CNI as the National Governmental CERT; trust in Incibe, the Spanish National Institute of Cybersecurity, and in the CNPIC, the National Centre for Infrastructure Protection and Cybersecurity, of the Ministry of the Interior", and instruct the Ministry of Defence to study the issue first, not to predetermine the model and to come up with a study along the lines of what has been proposed.

Ciudadanos also praised the proposal, although they highlighted a series of nuances that led them to disagree with the model proposed in the aforementioned legislative initiative, such as:

Volunteering, this kind of army of cyber-volunteers that you want to set up, is not the right way to approach this problem. I am not saying that it cannot be a complement. I believe that this is what the Government has to resolve, which is why we are not going to vote against this Non-Legislative Proposal. Still, we do urge the Government to offer us a solution as soon as possible, as the spokesperson for the Socialist Group has also mentioned, because I believe that the Government has to provide a solution to this.

Finally, the representative of Unidas-Podemos also agreed on the need to promote an initiative such as this, although he proposed doing so with caution and after a more in-depth analysis of the channels that should be used to achieve it. In this regard, he stated that:

In this regard, our group will call on the other groups to try to reach an agreement and to ensure that this initiative is neither frustrated nor carried forward without due caution.

Subsequently, in the session of the Congress of 26 July 2021, the Bureau of the Congress of Deputies admitted the transfer to the Government of the Draft Law for the Digital Transformation of Spain[24].

[24] Official Gazette of the Spanish Parliament (2021, 26 June). *Draft Law for the digital transformation of Spain*:
https://www.congreso.es/public_oficiales/L14/CONG/BOCG/B/BOCG-14-B-173-1.PDF

Article 60 of the bill includes the creation of a corps of reservists specialised in cybersecurity tasks, under the title "strategic reserve in cybersecurity" under the Ministry of Defence, where the purposes, conditions, deadlines and rights to form part of this corps are set out. By way of example, the most relevant points of this article are reproduced below:

> 2. Voluntary reservists belonging to the Strategic Reserve of Cybersecurity Talent will be Spaniards who, in accordance with the constitutional right and duty to defend Spain, and having applied to participate in the corresponding call, are selected to perform the functions assigned to them under the direction of the competent authorities of the Ministry of Defence, for the specific civil or military tasks indicated. These citizens will join the Armed Forces on a temporary and voluntary basis by means of a commitment of availability.
>
> 3. To form part of this specific reserve, the Defence Staff (EMAD), through the Joint Cyber Defence Command (MCCD), will select individuals who, due to their experience and technical or other expertise in the field, can contribute talent to the existing capabilities of the Armed Forces. The Strategic Cybersecurity Talent Reserve will report organically to the EMAD through the MCCD.
>
> [...]
>
> 7. Cyber volunteer reservists will be transferred to the service of the Armed Forces when they are activated. However, due to the special nature of their activity, they shall be on stand-by for the duration of their commitment. This means that, when necessary, they may be assigned to support cybersecurity tasks without the need to join their activation unit if circumstances make this necessary.
>
> 8. Periods of military service by reservists shall be considered as paid leave, subject to prior agreement with the company.

As can be seen, the cyber reserve proposal put forward in Spain is not only different in its approach to the proposal contained in the Cybersolidarity Act, although it can be considered complementary. Especially after the political declarations referred to in the opening paragraphs, which hint at the need for the civilian population to receive training in cyber defence, but also to be actively involved in actions to protect people and infrastructures. With regard to the latter, the Spanish proposal would also allow individuals who are not active in companies providing managed security services to collaborate in certain activities that could make the country's cyber defence schemes more effective at certain times.

More recently, in March 2024, the Partido Popular presented a new Non-Legislative Proposal to the Defence Committee of the Congress of Deputies, this time with the title "regarding the creation and regulation of the Strategic Talent Reserve in Cybersecurity under the Ministry of Defence to prevent cyberattacks on institutions in crisis situations". He justified this by stating that, at this time, there is an urgent need for a strategic cyber-defence reserve to combat external threats to our country and to any member of the European Union, of which we are a part.

In this regard, although this initiative has long been considered an ideal option for strengthening Spain's defensive capabilities, it is no less certain that, from the political sphere, there are conflicting positions, with certain parties opting to promote a figure of this nature, understanding it as a complement to the currently existing resources, while the current government considers that Spain already has sufficient resources to address the challenges of cybersecurity and that it would not be necessary to provide us with a corps of cyber-reservists.

6.1. CONCEPT.

The cyber reserve can be defined as a complementary force, composed of trained volunteer professionals from civilian, academic or public sector backgrounds, to assist in protecting against cyber threats in crisis or emergency situations.

The cyber-reserve proposal put forward by Spain is a concept similar to that of traditional military reserves, not focused on armed conflicts, but on defence against cyberattacks that, due to their seriousness and impact, reach a sufficiently serious level to be considered a threat to national security, in line with the spirit of the aforementioned European Regulation on cyber solidarity.

Individuals should possess specialised technical knowledge and skills, as well as advanced management skills in the field of cybersecurity. In short, it is a matter of complementing the resources available to the State concerned at any given time, aimed at protecting the country's most critical infrastructures.

6.2. COMPONENTS.

Cyber reserve volunteers are mostly citizens working in other professional fields (law, economics, sociology, anthropology, communication, etc.) outside the military or law enforcement agencies, who are willing to make their cybersecurity-related skills and knowledge available to their country in times of need.

Their participation may be temporary, and they may be called upon to respond to specific cyber incidents or participate in training exercises to maintain a high level of readiness.

6.3. OBJECTIVE.

The cyber reserve aims to strengthen the country's cybersecurity capabilities, as well as to provide a rapid and effective response to cyber incidents, in particular when they affect critical infrastructure.

Their creation and maintenance should be part of a nation's cyber security strategy, as their existence contributes to the resilience of businesses and the economy in general, and to all aspects of cyber security.

The cyber reserve should operate in coordination with other government entities with specific competencies in cybersecurity and national defence, such as cybersecurity agencies, the armed forces, law enforcement and response centres (CERTs and CSIRTs),

to ensure additional support during the public response to cyber threats that require such cooperation.

7. THE RESERVE AS PART OF NATIONAL CYBERSECURITY GOVERNANCE.

The cybersecurity reserve proposed in the Cybersolidarity Regulation should form part of the national cybersecurity governance model, as an instrument that should collaborate and coordinate with the rest of the State's security forces to maintain a capacity to respond to cyber incidents.

For the purposes of its dependence and responsibility for its constitution and development, there are several options, to be assessed in each case, and without prejudice to ENISA's involvement in the European reserve project supported by the cyber-solidarity regulation.

In Spain, the most appropriate bodies for the adoption of a body of this nature could be:

a. Ministry of Defence: Their involvement would involve effective strategic planning and coordination of the cyber reserve with other armed forces, ensuring that it is properly integrated into the overall national security strategy.

b. INCIBE: this entity often leads and coordinates cybersecurity efforts linked to the private sector (e.g., cybercooperants project[25]) and can play an important role in the creation and operation of the cyber-reserve. These agencies focus on detecting and preventing cyber threats, as well as working with other entities to ensure the protection of critical infrastructure and government systems.

c. Ministry of the Interior and police forces: Law enforcement agencies, both national and regional, can play a crucial role in cyber resilience, especially in the identification and prosecution of cybercriminals. They work closely with other agencies to conduct investigations and enforce the law in cybercrime cases.

d. Cyber Attack Response Centres (CERT/CSIRT): Cyber resilience can be linked to these centres, assisting in the early detection of incidents and coordination of the response.

e. Ministry of Digital Transformation: In some countries, the Ministry of ICT or equivalent entity may have a relevant role in the cyber reserve. Its participation is focused on guaranteeing the protection and security of information and communications technology infrastructures, which are fundamental to the country's functioning, although from a perspective far removed from the military and closer to civilian volunteering, which allows it to be more flexible in its management.

f. Private sector entities: The private sector should also be involved in cyber reserves, especially when recruiting reservists with specialised cyber security skills and knowledge. Collaboration with the private sector can provide a wide range of talent and

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

expertise, but without penalising the interests of the private entities that bear the costs of these professionals.

In view of these options, it would be up to the government to design the strategy it considers best to incorporate the cyber-reserve within the structure of the current cybersecurity governance framework, taking into account that direct dependence on public entities (such as, for example, the army or police forces) gives the cyber reserve a more rigid and formal character than if, for example, it is linked to bodies such as INCIBE or the Ministry responsible for digital competences.

8. INTEGRATION OF CYBER RESERVES INTO NATIONAL SECURITY STRUCTURES.

The integration of a future cyber reserve into national security structures implies collaboration with various government agencies and synchronisation of efforts to ensure a coordinated and coherent response to cyber incidents.

The process of achieving such integration, or at least acceptable coordination, requires the development of a series of actions, especially at the public level, to adapt the current cybersecurity governance and regulatory landscape to the effective development of such a body.

Prior to this, strategic planning should be developed that defines the long-term objectives of a cyber reserve and how they align with the national cyber security strategy. This planning should consider the required capabilities, areas of need and priorities of the cybersecurity reserve in the context of emerging threats.

Once this strategy is defined, one of the main actions to be considered is the adaptation of the current legal and policy framework to allow for a clear definition of the purpose, responsibilities, functions and authority of a civilian cyber reservist corps. Such an initiative implies the enactment of specific regulations establishing the basis for the creation and operation of the cyber reserve, as well as its collaboration with other governmental entities.

At the operational level, the integration of the cyber reserve requires adequate training and capacity building for its reservists. This may include cybersecurity training programmes, incident simulation exercises and training in the use of relevant tools and technologies. Ongoing training keeps reservists up to date and ready to respond to cyber threats.

As for the process of activation and deployment of such reinforcement, this requires establishing clear and agile processes for the activation and deployment of the cyber back-up in emergency situations. These processes should specify how members are called up, how they communicate and how their actions are coordinated with other entities involved.

Neither should it be forgotten that the successful integration of a cyber reserve also requires collaboration with the private sector. This may require cooperation agreements and sharing of cyber security best practices with companies and organisations operating critical infrastructures.

It is also important to periodically evaluate the effectiveness of cyber resilience and make adjustments and improvements based on lessons learned and new threats. Constant feedback will allow them to optimise their capabilities and ensure an effective response to the evolving challenges of cyberspace.

In summary, the integration of the cyber reserve into national security structures is a complex process that requires careful strategic planning, coordination with various government agencies and the private sector, and adequate training of reservists. With the right legal and policy framework, a well-integrated cyber reserve can be a valuable tool to strengthen the country's cyber security and protect it against cyber threats in the digital age, which, with the advent of artificial intelligence and, soon, quantum technologies, have shaped a more complex and sophisticated scenario that continues to make effective cyber incident management difficult.

9. THE PROFILE OF THE CYBER RESERVIST: SKILLS AND COMPETENCES.

The skills required of cyber reservists are critical to ensure that they can successfully meet the challenges posed by national crisis situations. These capabilities must be diverse and updated to adapt to constantly evolving technologies and cyber tactics. Notwithstanding the different cyber reservist profiles that may be defined, some of the key skills that members should possess include:

1. Knowledge of cybersecurity: Cyber reservists must have a solid knowledge of cybersecurity, an understanding of the fundamentals of computer security, network, system and application protection, as well as ethical *hacking* methodologies to understand how attackers think and act.

2. Threat analysis: It is essential that cyber reservists are able to analyse and understand emerging cyberthreats. They must be able to identify attack patterns, recognise malicious techniques and determine the severity and scope of incidents in order to respond appropriately. These skills would enable improvements to current intelligence and analytical capabilities.

3. Incident response: Cyber reservists should be trained in cyber incident management and response. This includes the ability to detect intrusions, contain and mitigate ongoing attacks, and conduct forensic investigations to determine the origin and nature of an incident. The contribution of cyber reservists in this field would improve incident identification and management capabilities, reinforcing technical response and mitigation capabilities.

4. Secure programming and development: A solid knowledge of programming languages and secure development is essential to identify and correct vulnerabilities in *software* and applications used in the country. This may involve the development of patches or solutions to mitigate security risks.

5. Cyberintelligence: Cyber resisters must be able to gather and analyse cyber intelligence to anticipate and counter potential threats. This involves tracking malicious actors, their infrastructure and tactics, and collaborating with other agencies to share relevant information. This reinforcement would improve Spain's preventive capabilities,

as well as increase knowledge of the attacks, the agents responsible, their motivations and, therefore, this information would allow Spanish companies and organisations to increase their resilience.

6. Effective communication: Effective communication is essential to coordinate efforts with other government entities, share relevant information and explain technical concepts in a way that is understandable to non-experts, especially citizens and entrepreneurs.

7. Critical thinking and problem solving: Cyber reservists must be critical thinkers and skilled problem solvers. They must be able to deal with complex and unfamiliar situations, make quick and effective decisions, and adapt to changing scenarios. This can enable new visions, perspectives and ways of managing threats to be incorporated, bringing added value to existing teams.

8. In-depth knowledge of the policy and regulatory environment. This, as in all other areas, would encourage the attraction and development of talent in these areas, as well as training and improvement of the regulatory environment, which is becoming increasingly complex and necessary.

9. Teamwork and collaboration: Cybersecurity is a collaborative effort that requires the ability to work as a team with other cybersecurity specialists, law enforcement and government agencies to address cyber challenges in a coordinated and effective manner. This could promote territorial cohesion, which is one of the objectives already included, for example, in the former National Strategy for Artificial Intelligence.

10. Ethics and responsibility: Cyber reservists must adhere to high ethical standards and be accountable for handling information and performing their duties. Confidentiality, integrity and accountability are fundamental to cybersecurity.

In short, cyber reservists must possess a diverse set of technical and other skills to meet today's cybersecurity challenges. Their expertise in cyber security, threat analysis, incident response and effective collaboration are essential to ensure a rapid and effective response to cyber incidents and protect the country's security and resilience in cyberspace.

10. POLICIES AND LAWS RELATED TO THE CYBER RESERVE.

The effective implementation of a cyber reserve, especially in the case of the Spanish proposal to create a corps of civilian volunteers, requires a solid legal and regulatory framework that establishes the rules and responsibilities for its operation. These policies and laws should be designed to ensure that a cyber reserve operates in a coordinated, efficient and legally and ethically sound manner.

The following are some key issues related to the regulation of cyber reserve:

a. Legislation of creation: countries that have established a cyber reserve (e.g. France) generally have specific laws or decrees authorising and defining its creation. Such legislation can establish the mission and purpose of the cyber reserve, as well as mechanisms for recruitment, training and activation in case of crisis.

b. Authority and coordination: policies and laws should specify the authority of the cyber reserve and how it will coordinate with other entities, such as the military, intelligence agencies, cybersecurity agencies and the private sector. It is important to establish a command and control structure to ensure a coherent and seamless response in the event of a cyber incident.

c. Data protection and privacy: cyber reserve activities often involve access to sensitive information and critical data. It is, therefore, vital that policies and laws establish safeguards to protect the privacy and confidentiality of information accessed by cyber reservists during their operations.

d. Use of civilian and private sector skills: Some cyber reserves incorporate private sector experts who have specialised skills in cybersecurity. Applicable national policies and laws should address how these reservists can be integrated and how potential conflicts of interest with their private employers will be handled.

e. Responsibilities and duties: Policies and laws should set out the responsibilities and duties of cyber reservists. This may include the obligation to keep their skills up to date, participate in training exercises and respond effectively to cyber incidents.

f. International coordination: in a highly interconnected world, the cyber reserve will address transnational challenges. Policies and laws should consider international cooperation and coordination with other cyber reserves or similar entities in other countries to address extraterritorial cyber threats.

g. Accountability and evaluation: the regulation should establish mechanisms to evaluate the effectiveness of the cyber reserve and ensure accountability. This may include periodic audits, activity reports and reviews to continuously improve response capabilities.

In general, policies and laws related to cyber reserve are essential to create a sound basis for its operation, ensure its effectiveness and protect national interests in cyberspace. These policies must adapt to changing cyber threats and challenges to ensure that cyber resilience remains relevant and capable of protecting the country's digital assets and critical infrastructure.

11. EXAMPLES OF COUNTRIES WITH A CYBER RESERVE.

1. United States[26].

The United States has what is known as the "*U.S. Cyber Reserve*". This body is composed of cybersecurity experts from different sectors, including government, private industry and academia.

[26] Brumfield, Cynthia (2024, 24 April). *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

Reserve members are trained to respond to cyber incidents and provide support in case of cybersecurity-related emergencies.

2. United Kingdom[27].

The UK established its *"UK Cyber Reserve*" to address the growing threat of cyberattacks. This cyber reserve is made up of cybersecurity specialists recruited from the private sector and the armed forces.

They work with the National Cybersecurity Centre (NCC) to protect the country's critical infrastructure and ensure national cybersecurity.

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

Estonia, a country known for its advanced approach to cybersecurity, has developed a cyber unit within the Estonian Defence League *(Kaitseliit*).

This unit aims to provide additional capability to defend against cyber attacks and contribute to the country's cyber resilience.

4. Singapore[29].

Singapore has established the *Singapore Armed Forces Cyber Defence Group* to address cyber threats and ensure the security of its information systems. The group is composed of highly qualified reservists with cybersecurity experience.

5. Israel -*Israeli Defence Forces Cyber Unit*[30].

Israel is known for its cyber security capabilities and has established a cyber unit within the Israel Defence Forces (IDF). The unit focuses on cyber defence, intelligence and countering cyber threats facing the country.

Israel tailors its cyber reserve approach and structure according to its specific needs and the nature of the cyber threats it faces.

6. France - "*Réserve Citoyenne Cyberdéfense*"[31].

The cyber reserve in France, known as the "Citizen Cyber Defence Reserve", is a programme launched by the French government to mobilise civilian experts in

[27] UK Government (2024, June). *Joint Cyber Reserve Force.* https://www.gov.uk/government/groups/joint-cyber-reserve-force
[28] Estonian Ministry of Defence (2024, June). *Cyber Command.* https://mil.ee/en/landforces/cyber-command/
[29] Ministry of Defence of Singapore (2024, June): https://www.mindef.gov.sg/web/portal/mindef/home
[30] Israeli Ministry of Defence (2024, June). *C4i and Cyber Defence Directorate.* https://www.idf.il/en/mini-sites/directorates/c4i-and-cyber-defense-directorate/c4i-and-cyber-defense-directorate/
[31] French Ministry of the Armed Forces (2024, June). *La réserve.* https://www.defense.gouv.fr/comcyber/nous-rejoindre/reserve

cybersecurity and information technology to strengthen the country's cyber defence. This programme is part of France's broader efforts to protect itself against cyber threats and strengthen its cyber resilience.

The Cyber Defence Citizen Reserve was created in 2014, and is open to French citizens with skills and experience in areas related to cyber security, such as information security, digital forensics, incident management, and network and system protection, among others. The main objective of this initiative is to provide an additional and complementary resource to the cyber defence capabilities of the government and the armed forces.

Cyber defence reservists are involved in activities such as detecting and responding to cyber incidents, assessing vulnerabilities in computer systems, cyber security awareness and education, and research and development in security technologies. They can also be mobilised in the event of a cyber crisis or large-scale cyber attack to support the government's defence and response efforts.

Spain could gain valuable knowledge from the experience of such countries, and reinforce the exchange of information and design exchanges of professionals that would allow them to increase their level of training and knowledge in cybersecurity and, in particular, in the prevention and management of cyber attacks.

12. CONCLUSIONS.

The Cybersolidarity Act will create a European cybersecurity reserve to provide the European Union with resources to improve its cyber defence capabilities against high-impact incidents. This is an opportunity for Spain to train and attract talent in a sector that is increasingly in need of qualified professionals.

This new line of cyber defence, called *cyber shield*, will be organised through a network of public SOCs and privately managed security service providers, which will provide highly skilled professionals and cyber security expertise to address threats that exceed normal defence capabilities.

Without prejudice, and complementary to this initiative, some countries have designed a corps of cyber-reservists, composed of civilian personnel with experience in managing cyber-security incidents in the business and academic worlds, who can bring their knowledge and experience to help complement the capabilities of the relevant public services in this field, with the aim of improving national resilience to growing and increasingly sophisticated cyber threats.

In this case, in order to meet the new needs for awareness-raising and training of the civilian population in the defence of public and private networks and systems and the information stored in them, digital assets and infrastructures in general, it is necessary to design and implement a corps of volunteer reservists who are experts in the field, who can provide occasional and extraordinary support at certain times.

In order to design a corps of this nature, Spain has ample experience in organising a corps of reservists, so the design of a corps of cyber-reservists can be considered in addition to and complementary to the current capabilities of the national cybersecurity

reserve, as well as coordinated with the other cyber-reserve corps of other countries. All these are benchmarks in the field of cybersecurity and have been able to take advantage of this initiative to develop a robust industry in this area, as well as an outstanding geostrategic positioning in this field of national security.