BRIEFING

EU Legislation in Progress

New European cybersecurity competence centre and network

OVERVIEW

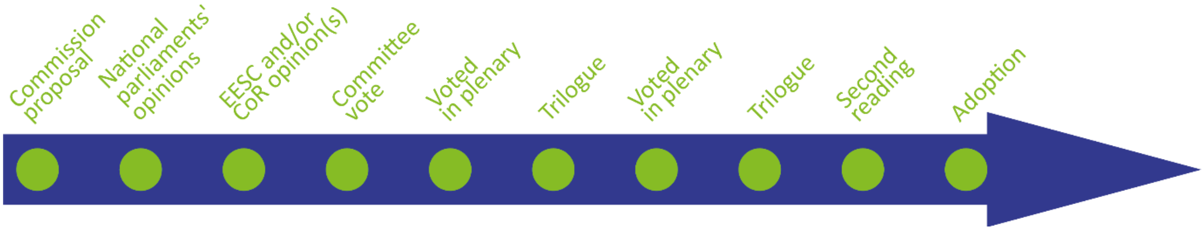
On 13 September 2017, the Commission adopted a cybersecurity package with a series of initiatives to further improve EU cyber-resilience, deterrence and defence. A year later, the Commission presented a proposal for the creation of a European cybersecurity competence centre with a related network of national coordination centres. The initiative aimed to improve and strengthen the EU's cybersecurity capacity, by stimulating the European technological and industrial cybersecurity ecosystem as well as coordinating and pooling necessary resources in Europe.

The competence centre was supposed to become the main body that would manage EU financial resources dedicated to cybersecurity research under the two proposed programmes – Digital Europe and Horizon Europe – within the next multiannual financial framework, for 2021-2027.

Within the European Parliament, the file was assigned to the Committee on Industry, Research and Energy (ITRE). The report was adopted on 19 February 2019 in the ITRE committee. On 17 April 2019 the Parliament adopted its position at first reading, after two trilogue meetings, before the European elections. A new trilogue meeting took place more than a year later, on 25 June 2020, and further negotiations followed. During the fifth trilogue meeting on 11 December 2020, the negotiators of the Council and the European Parliament reached a provisional agreement. The Council adopted the legislation in April 2021 at first reading. The ITRE committee made its recommendation for second reading in April 2021, and Parliament adopted the text during the May 2021 plenary session. It entered into force on 28 June 2021.

Proposal for a regulation establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres

Committee responsible:	Industry, Research and Energy (ITRE)	COM(2018) 630
Rapporteur:	Rasmus Andresen (Greens/EFA, Germany)	12.9.2019
Shadow rapporteurs:	Pilar Del Castillo Vera (EPP, Spain) Jens Geier (S&D, Germany) Claudia Gamon (Renew, Austria) Evžen Tošenovský (ECR, Czechia) Marc Botenga (The Left, Belgium)	2018/0328(COD) Ordinary legislative procedure (COD) (Parliament and Council on equal footing – formerly 'co-decision')
Procedure completed	Regulation (EU) 2021/887 OJ L 202, 8.6.2021, pp. 1-31	



EPRS | European Parliamentary Research Service

Author: Mar Negreiro with Alessia Belluomini and Polona Car
Members' Research Service

PE 635.518 – May 2024

EN

Introduction

Critical sectors, such as transport, energy, health and finance, have become increasingly dependent on digital technologies to run their core business. While growing digital connectivity brings enormous opportunities, it also exposes the economy and society to cyber-threats. The number, complexity and scale of cybersecurity incidents are growing, as is their impact on the economy and society. This trend is expected to increase further, in parallel with technological developments, such as the proliferation of devices linked to the Internet of Things (IoT). In an increasingly connected world, where 41 billion IoT devices are expected to be in use by 2025, the growing challenges in the cybersecurity landscape have led the EU to reflect on how to enhance the protection of its citizens and companies against cyber-threats and attacks.

According to a survey conducted by the European Commission in 2023 77 % of EU citizens feel the need for greater cybersecurity and safety of digital technologies to facilitate their daily use. Moreover, respondents list the protection of users from cyberattacks as the EU citizens' top priority for future actions in their countries. A 2023 ENISA report on the threat landscape in the EU revealed that cyber criminals spared no sector, with the public administration and health care being the two most frequently targeted. These attacks are becoming increasingly severe, complex and inexpensive to launch and are inducing losses worth billions of euros per year.

It is therefore no surprise that cybersecurity products and services constitute an important and rapidly growing market. There, however, Europe faces strong competition from the United States and Asia; a Commission analysis attributes this to the fact that even though a lot of innovative cybersecurity research is taking place in Europe, its results are rarely commercialised.

According to the above analysis, even though the EU retains a wealth of expertise in cybersecurity, it is not fully exploited: a 2018 report by the Commission's Joint Research Centre (JRC) highlighted that this expertise, if transformed into marketable products and solutions, could allow the Union to cover the whole cybersecurity value chain. According to the Commission, the cybersecurity industry in Europe had developed largely on the basis of national government demand, including for defence. Meanwhile, companies still found it difficult to grow beyond the boundaries of their national markets due to the divergent rules that governed them. As a consequence, while these companies tended to be strong and innovative, they were smaller in size in comparison to their US, Israeli, Chinese, and South Korean counterparts. The analysis concluded that without policy intervention to address the fragmentation of European efforts and innovation capacities, the European cybersecurity industry might not be capable of taking advantage of its potential or competing with other global players.

Europe also faces a shortage of skilled cybersecurity professionals. According to Commission estimates, the cybersecurity workforce gap in Europe ranged between 260 000 and 500 000 in 2022, while the EU's cybersecurity workforce needs were estimated at 883 000 professionals. Last but not least, the Commission pointed out in 2018 that the lack of coordination of cybersecurity research and innovation efforts was also resulting in a brain drain, pushing talented researchers to look for opportunities outside the EU. It stressed that the research and industrial communities, as well as the public sector, in Europe were struggling as a result of insufficient capacity and access to the facilities needed to carry out cybersecurity experiments, tests and operations, which were often too costly.

Existing situation

The first step towards the creation and development of an EU cybersecurity ecosystem was the adoption of a cybersecurity strategy in 2013, laying out the principles and goals for a Union-wide cybersecurity policy. The strategy identified the achievement of cyber-resilience and the development of industrial and technological resources for cybersecurity as its key objectives.

The Directive on Security of Network and Information Systems across the EU (the NIS Directive), in force since 9 May 2018, represents the first piece of EU-wide legislation on cybersecurity. It provides for legal measures to boost the overall level of cybersecurity in the EU with a focus on protecting critical infrastructure. Among other things, it established the NIS cooperation group, to ensure strategic cooperation among Member States, and the network of computer security incident response teams (CSIRTs), to ensure both the exchange of information on cybersecurity and cooperation on specific cybersecurity incidents.

In its 2016 communication on strengthening Europe's cyber-resilience system and fostering a competitive and innovative cybersecurity industry, the Commission assessed the opportunities for the cybersecurity industry in Europe and announced, among other things, some measures to advance the EU's cybersecurity research and innovation.

In the 2017 mid-term review of the digital single market strategy, the Commission identified tackling cybersecurity threats as one of the key priorities for the years to come. On 13 September 2017, the then European Commission Vice-President and EU High Representative for Foreign Affairs and Security Policy, Federica Mogherini, presented a joint communication entitled 'Resilience, deterrence and defence: Building strong cybersecurity for the EU'. The proposed initiatives in this cybersecurity package included setting up a European cybersecurity competence centre (hereafter referred to as the Competence Centre) and a network of national coordination centres (hereafter referred to as the Network). It also included a proposal for a 'Cybersecurity Act' regulation, which has since been adopted. It enforces the role of ENISA, the EU cybersecurity agency while also establishing a voluntary cybersecurity certification framework in the EU.

Under the previous multiannual financial framework (MFF), for 2014 to 2020, EU funding for cybersecurity was channelled through a number of programmes and funds. For instance, the EU research programme Horizon 2020 invested roughly €600 million in cybersecurity projects (an additional €450 million was devoted to the public-private partnership on cybersecurity (cPPP[1]) over the 2017-2020 period); under the European structural and investment (ESI) funds, up to €400 million was allocated for investment in trust and cybersecurity; the Connecting Europe Facility (CEF) invested about €30 million in cybersecurity measures in the 2014-2017 period.

Cybersecurity remained a priority area for further action for the European Commission and for the Council for the 2019 to 2024 period under the EU digital strategy. The COVID-19 pandemic saw an increase in malicious cyber-activity across EU Member States. Criminals exploited the crisis to their own advantage, as revealed by a Europol report. Likewise increased e-commerce and cashless payments have brought a heightened risk of cybercrime attacks and cybersecurity breaches. Over 87 % of EU citizens consider cybercrime an important challenge: with payments becoming increasingly cashless, online theft – of money and also of personal data – has been on the rise. That it is why it was included as one of the areas for action under the COVID-19 recovery plan.

For the 2021-2027 programming period, EU cybersecurity initiatives and support activities are being funded through a mix of different instruments and strands, such as the Digital Europe programme, Horizon Europe and the European Defence Fund.

Parliament's starting position

Already in its resolution of 12 September 2013 on the 'Cybersecurity strategy of the European Union: An open, safe and secure cyberspace', the European Parliament called for the development of cyber-resilience for critical infrastructure as one of a number of measures to counter the growing cyber-security challenges.

In its resolution of 19 January 2016, Towards a digital single market, the Parliament called for efforts to improve EU resilience to cyber-attacks, pointing out that this could be achieved by means of increasing the relevant financial and human resources and ensuring cooperation between the European cybersecurity industry, the public and the private sector.

In its resolution of 13 June 2018 on cyber-defence, the European Parliament welcomed the Commission's 2017 cybersecurity package and called, among other things, for the EU and the

Member States to give more practical support to the European cybersecurity industry to reduce dependencies on cybersecurity products from external sources. It also encouraged the Commission to integrate cyber-defence elements into a network of European cybersecurity competence and research centres, with a view to providing sufficient resources for dual-use cyber-capabilities and technologies within the next MFF.

Council and European Council starting position

The Council of the EU has stressed the importance of increased resilience to prevent and respond to cyber-threats across the EU. In its conclusions of November 2017, the Council underlined the need for the EU, its Member States and the private sector to ensure sufficient financing for enhancing cyber-resilience, supporting cybersecurity research and stepping up development efforts across the EU. To this end, it welcomed the cybersecurity package presented by the Commission on 13 September 2017, including its intention to set up a network of cybersecurity competence centres, and called on the Commission to rapidly provide an impact assessment for the development of a legislative proposal related to the package.

Following the submission of the cybersecurity package, in its conclusions of 24 October 2017, the Council agreed to set up an action plan for EU cybersecurity reform. EU leaders regarded cybersecurity reform as one of the key conditions for completing the EU digital single market; accordingly, they called for a determined R&D and investment effort.

In its conclusions of 18 October 2018, the European Council called for further measures to build strong cybersecurity and to strengthen EU resilience against cyber-attacks. It also called for negotiations on all cybersecurity proposals to be concluded before the end of the 2014-2019 legislature.

In its conclusions on the EU cybersecurity strategy from 22 March 2021, the Council called for the rapid set up and operationalisation of the European Cybersecurity Competence Centre and for the prompt adoption of its agenda to strengthen the EU strategic autonomy and support technological capacities and skills development for the industry and academic communities, including SMEs and research centres.

Preparation of the proposal

To prepare the current proposal, the Commission conducted a dedicated study, held workshops with key stakeholders and carried out an impact assessment. The Commission did not launch a public consultation on the proposal.[2]

In support of the initiative, in 2018 the JRC prepared a study looking at the scope and definitions of cybersecurity. In a related survey, it gathered input from 655 cybersecurity expertise centres located in the EU, describing their activities, working fields and international cooperation.

The study provided evidence showing that in terms of scientific production, the EU is the second most relevant cybersecurity player in the global research arena (after the US). In the patenting domain, however, the EU has less relevance due to its weak capacity in fostering (long-term) collaboration between industry and academia.

The results of the survey showed that Horizon 2020 has contributed to strengthening relations between industry and academia; however, an analysis of the participants' profiles shows that only a few institutions have gained access to funds allocated under the programme and succeeded in doing so on a continuous basis. As a result, polarisation with regard to cybersecurity research has occurred, whereby only a few institutions in a small number of Member States have received programme support, while the remaining institutions across the EU have benefited more from national funding programmes with limited international collaboration.

Furthermore, the survey results show the limitations of the European cybersecurity research community, which lacks the coordination necessary to create synergy and is not always able to cooperate closely with industry.

Two stakeholder workshops were organised with representatives of the national competence centres, national authorities and industry. At the first, held on 23 February 2018, the Commission invited the European cybersecurity expertise centres to exchange views on possible ways of reinforcing EU cybersecurity research capabilities and on improving the coordination of research and innovation efforts with industrial partners. A second workshop was held on 22 March 2018, where players from industry and the research community, alongside representatives of the Member States, discussed the initiative on establishing a cybersecurity competence centre and a supporting network of national competence centres.

Afterwards, the Commission invited the main EU bodies concerned – the European Network and Information Security Agency (ENISA) and the European Defence Agency (EDA) – to give their input to the consultation process:

- The EDA drew attention to its work promoting capability development in the field of cyber-defence through intergovernmental cooperation among the Member States. It pointed out that development of cross-sectoral research agendas, identification of areas where civil/military efforts and investments should be combined, development of common training and exercises curricula and the conduct of coordinated or joint cyber activities, could be some of the topics to which a future Competence Centre and Network could add value.
- ENISA welcomed the Commission's proposal and strongly supported its goal of increasing coordination and enhancing cybersecurity competencies within the EU. According to the agency, the Competence Centre and Network should focus on the following priorities: developing the strategy and governance system, identifying its short/long-term objectives; developing and maintaining digital skills throughout the EU, and prioritising technical work.

In March and April 2018, the Commission met for a targeted consultation with the management board of the European Cybersecurity Organisation (ECSO) and the cPPP.

The impact assessment accompanying the proposal was presented on 12 September 2018. Citizens and stakeholders were offered the possibility to give feedback (see the section on 'Stakeholders' views'). Three preliminary policy options were considered:

- Option 0: Baseline scenario (status quo). This 'collaborative option' assumed the continuation of the current policy approach to managing cybersecurity research and industry policy in the EU throughout the next framework research programme, based on the continuation of the cPPP and the cooperation among expertise centres promoted by the Commission through the launch of a pilot project;
- Option 1: the creation of a Competence Centre and Network empowered to pursue measures in support of industrial technologies and measures in the domain of research and innovation;
- Option 2: the creation of a Competence Centre and Network limited to research and innovation activities only.

Among the three options retained for in-depth assessment, it was concluded that option 1 was the most suitable for achieving the goals of the initiative, as it would help to create a real cybersecurity industrial policy by supporting activities related not only to research and development but also to market deployment. This option would ensure flexibility to allow the application of different models of cooperation within the Network. This would optimise both the use of existing knowledge and resources, and the ability to structure cooperation and joint commitments of the public and private stakeholders coming from all relevant sectors, including defence. Furthermore, option 1 allows to increase synergies while also offering an implementation mechanism for two different EU cybersecurity funding streams under the next MFF: the Digital Europe and the Horizon Europe programmes.

The European Parliamentary Research Service (EPRS) prepared an initial appraisal of the impact assessment. The appraisal found that the Commission's impact assessment set out the issue logically, but that the options examined were limited, due to a number of parameters being set in advance, and which may have restricted the scope of the impact assessment.

The changes the proposal would bring

The draft regulation proposed to create a new EU structure to pool and share cybersecurity research capacities and outcomes in a domain where EU capabilities and competences are considerable but still fragmented.

The new structure described in the proposal – an EU-level Competence Centre with its Network of national-level competence centres – would apply a comprehensive approach supporting cybersecurity across the entire value chain, from research to the deployment and uptake of key technologies.

On the one hand, in the spirit of the proposal the Competence Centre would facilitate and help to coordinate the work of the Network and nurture the cybersecurity competence community[3] by driving the cybersecurity technological agenda and facilitating access to existing expertise.

On the other hand, the draft regulation aimed to foster regular dialogue with the private sector, consumer organisations and other relevant stakeholders, enabled by the set-up of an industrial and scientific advisory board that would build on and scale up the effect of the existing cPPP on cybersecurity.

The Competence Centre, together with the Network, would also work towards supporting research to facilitate and accelerate standardisation and certification processes, in particular those related to cybersecurity certification schemes within the meaning of the Cybersecurity Act.

Furthermore, the proposal assigned to the Competence Centre the task of enhancing synergies between the civilian and defence dimensions of cybersecurity with regard to research, development and deployment. It should support Member States and other relevant actors by providing advice, sharing its expertise and facilitating collaboration on common projects and actions. When asked by Member States, it could also act as a project manager, notably in relation to the European Defence Fund.[4]

In addition, the draft regulation aimed to address the skills gap in cybersecurity by supporting skills development policies and training.

The planned governance structure of the Competence Centre included a governing board, an executive director, and an industrial and scientific advisory board.

The principal decision-making body would be the governing board, in which all Member States would take part but voting rights would be reserved for those making financial contributions. The Competence Centre would be funded jointly by the EU and the Member States. In view of its responsibility for the EU budget, the Commission would hold 50 % of the votes. The governing board would be assisted by an industrial and scientific advisory board to ensure regular dialogue with the private sector, consumer organisations and other relevant stakeholders. Each Member State would nominate the entity to act as its national coordination centre within the Network. These centres would support the Competence Centre in achieving its objectives and, in particular, in coordinating the cybersecurity competence community, while also facilitating the participation of industry and other actors at Member State level in cross-border projects.

The Competence Centre and its Network would act as an additional support to existing cybersecurity policy provisions and actors; its mandate would be complementary to ENISA's efforts.

The Competence Centre would become the main implementation mechanism for activities in support of the cybersecurity industry (including deployment, investment and research) under both Horizon Europe and Digital Europe in the next MFF (2021-2027).

The proposal entitled the Competence Centre to implement relevant parts of the two programmes by allocating grants, enhancing coherence and synergies between them, and carrying out procurements. For this purpose, the Commission proposed to allocate nearly €2 billion from Digital Europe for the 2021-2026 period and €2.8 billion from Horizon Europe for setting up the Competence Centre.

These substantial resources reflect the EU's commitment to investing more in cybersecurity policy. The proposal aimed to create synergies between funding programmes and tools for cybersecurity-related research and innovation both in civilian and defence areas. In fact, the proposal entitled the Competence Centre also to manage EDA resources, which would complement those earmarked under Horizon Europe.

Advisory committees

The European Economic and Social Committee (EESC) adopted an opinion on this proposal on 23 January 2019, prepared by its Section for Transport, Energy, Infrastructure and the Information Society.

The EESC welcomed the Commission's initiative, considering it an important step in developing an industrial strategy for cybersecurity and a strategic move to achieve robust and comprehensive EU digital autonomy. It also considered that the sensitive aspects related to governance, funding and achieving the objectives set should be outlined in advance.

The EESC was in favour of increasing the partnership model to a tripartite one featuring industry alongside the Commission and the Member States. However, it also stressed that such a partnership should be underpinned by a robust mechanism to prevent the involvement of non-EU companies that risk undermining the EU's security and autonomy.

The Committee considered it important to set out the details of the cooperation arrangements and relations between the Competence Centre and the Network. It believed it also important that the national centres be funded by the EU. Some concerns were raised on how the Competence Centre would be involved in coordinating the Digital Europe and Horizon Europe funding streams, or what guidelines would be followed when framing and awarding contracts to avoid duplication and overlaps. Furthermore, in order to increase the volume of the budget, the EESC suggested increasing synergies with other EU financial instruments (e.g. regional funds, structural funds, the CEF, the European Development Fund, the InvestEU programme). It further requested clarification of the respective remits and collaboration mechanisms with related agencies such as ENISA, the EDA, Europol and the CERT-EU network.

The European Committee of the Regions (CoR) was not required to adopt an opinion. However, in its opinion on the digital single market mid-term review (30 January 2018), it stressed that the Commission's new cybersecurity strategy should help improve the prevention and detection of and response to cyber incidents.

National parliaments

The deadline for national parliaments to submit their reasoned opinions on the grounds of subsidiarity was 13 November 2018. None were submitted, but three Member States made contributions.

- The Portuguese Assembleia da República adopted a written opinion on 31 October 2018, concluding that the proposal complies with the principle of subsidiarity.
- The Spanish Cortes Generales adopted an opinion, in which it welcomed the initiatives but pointed out that the proposal does not explain what functions the Competence Centre would have.
- In its position, the Romanian Senate made some remarks on the Competence Centre's proposed voting system, which links the right to vote to the making of national financial

contributions to the centre. More specifically, it argued that all Member States should be entitled to vote, given that they all contribute to the financing of the Commission on an ongoing basis.

Stakeholder views[5]

From 26 March to 23 April 2018, all interested stakeholders could provide feedback on the inception impact assessment on a dedicated Commission webpage. The Commission received a total of 22 responses, from the private sector, research organisations and citizens as well as one association from a third country.

Stakeholders pointed to the need to share the cost of investing in research equipment, which is often priced beyond the reach of many organisations, be they public or private. Furthermore, stakeholders emphasised the need for focused action to stimulate a dual approach, allowing civil and military stakeholders to interact in the development of a new security technology.

The Basque Cybersecurity Centre supported the establishment of the Competence Centre and Network and the exclusion of military research from this framework, so as to ensure technology neutrality. The centre suggested applying a regional ecosystem approach that supports innovation hubs.

The Communication Department at the University of Münster (Germany) called for a focus on multifaceted and interdisciplinary research in both computer science and the social sciences.

Eurosmart, the association representing the European digital security industry, welcomed the Commission's initiative, yet expressed its support for keeping the cPPP.

T&D Europe, the European association of electricity grid technology providers, raised concerns about the governance structure and recommended a set-up drawing on pre-existing national associations, in order to avoid 'multi-layered communities'.

Microsoft focused on two priority issues: first, to ensure that the European cybersecurity centre delivers relevant research, it needed to keep pace with the fast-moving technological development; and second, when formulating priorities, actions and strategy, the centre needed to apply a market-driven approach requiring the involvement of tech companies.

Danish air navigation service provider, Naviair, considered the current coordination as being rather fragmented, since there were too many players on the scene and there was duplication of efforts. Therefore, the creation of yet another centre would not render cooperation more seamless. That said, Naviair favoured the creation of a joint undertaking that would help establish 'clear governance'.

Siemens supported the approach presented and encouraged the exchange of views with the Network of national competence centres. It also called for industry to be adequately represented and involved when planning the content of research and innovation programmes.

Legislative process

Within the **European Parliament**, the file was assigned to the Industry, Research and Energy Committee (ITRE) (rapporteur: Julia Reda, Greens/EFA, Germany). The Internal Market and Consumer Protection Committee (IMCO) and the Budgets Committee (BUDG) were appointed as committees for opinion. Subsequently, BUDG decided not to give an opinion

The IMCO opinion was adopted on 31 January 2019. It supported the Commission's proposal while also calling for a number of improvements. Among other things, it asked for the application of consistent accreditation and assessment processes when selecting the members of the cybersecurity competence community. It also proposed a balanced representation of stakeholders in the Competence Centre, insisting that particular attention be given to the inclusion of SMEs. In terms of the Competence Centre's funding, IMCO believed the Commission should not have the power to terminate, proportionally reduce, or suspend the EU's financial contribution to the Competence Centre in the event that a contributing Member State did not contribute as expected.

On 7 December 2018, the rapporteur presented the draft report, discussed during the ITRE committee meeting of 14 January 2019. The deadline for amendments was 16 January 2019. A total of 113 amendments to the proposal were put forward. The report was adopted in the 19 February 2019 ITRE committee meeting, and then debated and voted by Parliament during the March I 2019 plenary session.

The report welcomed the Commission's initiative and underlined the role of ENISA, which should be consulted on all of the Competence Centre's relevant activities, as a way to create synergies. The report further stressed the need to ensure that European industrial players seize the opportunities and make use of the strengths the cybersecurity sector can provide. Among these players are small and medium-sized enterprises (SMEs), which contribute substantially to innovation, creation of products and processes, and provision of services in the field of cybersecurity. In addition to SMEs, it should also consider including individual experts, such as those coming from civil society and academia, in the cybersecurity competence community. The report shifted the proposal's focus to ICT products and services as 'solutions' that can guarantee security, to one where security is understood as a process that is constantly reassessed and strengthened throughout the lifecycle of a product or service.

The report incorporated free and open-source software into the scope of the proposal. It pointed out the crucial role such software plays for the functioning of our common infrastructure, the internet, from the provision of its basic infrastructure layer up to the applications with which users interact. Consequently, the report argued, in order to enhance the overall reliability, resilience and security of the internet, the centre should recognise the role of commonly used free and open-source software and contribute to its security.

The report pointed out the importance of limiting the Competence Centre's activities to civilian purposes. The Competence Centre should not facilitate any defence research or other defence-related projects, as its structure and functions would be financed by EU programmes that may not be used for military purposes. It goes on to add that where ICT security products and processes can be equally useful in civilian and military contexts ('dual-use products'), 'the [Competence] Centre should support existing frameworks for the control of dual-use technologies'.

The report also recognised the need to address the existing cybersecurity skills gap and ensure that the ICT community of workers is more gender and ethnically balanced, and recruits more persons with disabilities. In terms of improving its governance, the Competence Centre should avoid conflicts of interest; whenever such occur, it should handle them in a transparent and accountable manner. The Member States should apply this same principle to the governance of the national coordination centres. The report specified that ENISA should continue to fulfil its strategic objectives especially in the field of cybersecurity certification as defined in the Cybersecurity Act, while the Competence Centre should act as an operational body in cybersecurity and that ENISA should be consulted on the Competence Centre's relevant activities.

The report limited the Industrial and Scientific Advisory Board to no more than 25 members, including only representatives of entities which are not controlled by a third country or a third country entity (EEA and EFTA countries excepted). The Board's composition should aim to achieve gender balance, and include a balanced representation of the stakeholder groups from industry, academic community and civil society. In addition the report proposed that the Governing Board include one representative of each Member State, one representative nominated by the European Parliament as an observer, and four representatives of the Commission, on behalf of the Union, also aiming to achieve gender balance among board members and their alternates. ENISA and the Industrial and Scientific Advisory Board, should be permanent observers in the Governing Board, in an advisory role without voting rights.

In the **Council**, 15 Member States provided written comments on the proposal by the deadline of 8 November 2018. According to the progress report published on 23 November 2018, most delegations supported the general objectives of the proposal, in particular the need to retain and develop the cybersecurity technological and industrial capacities necessary to secure the digital single market, and to increase the competitiveness of the EU's cybersecurity industry, especially by deepening the coordination of the Union's cybersecurity research programmes. However, a number of concerns and questions were raised with regard to the governance structure: further clarification was demanded on the details of the implementation structures and financing mechanisms, and on the demarcation line and synergies with existing structures.

Two **trilogue meetings** took place on 13 and 20 March 2019. However, given the short timeframe until the end of the parliamentary term, the co-legislators did not have enough time to come to an agreement. A number of **pending questions were still to be agreed**, as the outgoing rapporteur, Julia Reda (Greens/EFA, Germany), explained during the last ITRE meeting of the previous legislative term on 2 April 2019. Among them was a need for further clarification on the tasks, governance structure, implementation structures and the financing mechanisms, given that two different funding programmes are involved (Horizon 2020 and Digital Europe), and the Member States' contributions were not yet decided. Similarly, this was a new type of structure which had not yet been tested and therefore needed further consideration.

Parliament adopted its position at first reading during the April II 2019 plenary session. Following the May 2019 elections, in the new Parliament the ITRE committee voted in favour of negotiations with the Council on the basis of the first-reading position, and appointed Rasmus Andresen (Greens/EFA, Germany) as new rapporteur.

In the Council, a new mandate for negotiations with the European Parliament was agreed by Coreper on 3 June 2020, under the Croatian Presidency. A third trilogue meeting then took place on 25 June 2020 – more than a year after the previous meeting in March 2019.

During the ITRE committee meeting on 6 July 2020, the rapporteur gave details of the latest trilogue meeting negotiations with the Council and explained some of the main issues at stake: the EU role in developing cybersecurity in the competence centre remained to be clarified. Parliament would like the competence centre mandate broadened: apart from distributing funds to participants from the Digital Europe and Horizon Europe programmes, it should also actively develop and support open source and standardisation. Parliament was also in favour of formally adding civil society and businesses organisations to the structure of the advisory board of the competence centre. Other remaining issues such as voting rights and the location of the seat were also still to be decided.

On 19 October 2020, the regulation was included in the Commission Work Programme 2021 (Annex III) as one of the priority pending proposals.

On 29 October 2020, the fourth trilogue meeting took place. The rapporteur briefed the ITRE committee during its meeting of 12 November 2020.

Meanwhile the procedure for the selection of the seat of the centre was launched by the Council on 28 October 2020. Bucharest, Romania was selected by representatives of the governments of the Member States as the seat of the new European Cybersecurity Industrial, Technology and Research Competence Centre.

On 11 December 2020, the negotiators for the Council and the Parliament reached a provisional agreement during the fifth trilogue meeting. Coreper approved the provisional agreement on 18 December 2020. On 14 January 2021, the ITRE committee voted in favour of the provisional agreement reached in trilogue, with 69 votes in favour to 3 against, and 4 abstentions.

The Council adopted the legislation creating the Centre and the Network of National Coordination Centres on 20 April 2021, at first reading. In the European Parliament, the ITRE committee adopted its recommendation for second reading in its meeting on 26 April 2021, with 64 votes in favour, 1 abstention and 10 against. The Commission published a summary of the main points in the negotiation, stating that it had accepted the position of the Council, which reflected the agreement reached in trilogue. The most important changes regarding the initial Commission proposal concerned voting rights and co-financing. The Commission regretted that Member States' contributions were not specified as part of the regulation, but were termed 'voluntary' contributions. According to the Commission this did not demonstrate the long-term commitment of all parties involved.

Parliament adopted the text on 19 May 2021 at second reading without a vote and it was signed by both co-legislators on 20 May 2021. It was published in the Official Journal on 8 June 2021 and entered into force on 28 June 2021. The new centre opened its doors on 8 May 2023.

EUROPEAN PARLIAMENT SUPPORTING ANALYSIS

Car P., Cyber solidarity act, EU Legislation in Progress, EPRS, European Parliament, February 2024.

Kononenko V. with Stenstrom R., Establishing the Cybersecurity Competence Centre and the Network of National Coordination Centres, Initial appraisal of a European Commission Impact Assessment, EPRS, European Parliament, February 2019.

Szczepański M., Digital Europe programme. Funding digital transformation beyond 2020, EU Legislation in Progress, EPRS, European Parliament, February 2019.Negreiro M., ENISA and a new cybersecurity act, EU Legislation in Progress, EPRS, European Parliament, July 2019.

Cybersecurity in the EU Common Security and Defence Policy (CSDP): Challenges and risks for the EU, study, Scientific Foresight Unit (STOA), EPRS, European Parliament, 2017.

OTHER SOURCES

European Cybersecurity Industrial, Technology and Research Competence Centre and Network of National Coordination Centres, European Parliament Legislative Observatory (OEIL).

Special Eurobarometer: Europeans' attitudes towards cyber security, European Commission, September 2017.

Building an effective European cyber shield. Taking EU Cooperation to the Next Level, EPSC Strategic Notes, European Political Strategy Centre, May 2017.

Cybersecurity in the Digital Single Market, High Level Group of Scientific Advisors, Scientific Opinion No 2/2017.

European Cybersecurity Centre of Expertise - Cybersecurity Competence Survey, Joint Research Centre, European Commission, 2018.

ENDNOTES

[1] The partnership, which includes the European Commission and a number of key stakeholders in the cybersecurity market represented by ECSO, was created with the purpose to gather industrial and public resources to deliver excellence in research and innovation and maximise the use of available EU funds through greater coordination with Member States and regions.

[2] However, the topic of cybersecurity was partially covered by two other open public consultations that ran from 10 January to 9 March 2018: the first focused on security, defence and crisis/emergency response, and the second focused on investment, research and innovation, SMEs and the single market.

[3] The cybersecurity competence community would consist of industry, academic and non-profit research organisations, and associations as well as public and other entities dealing with operational and technical matters. It would bring together the main stakeholders with regard to cybersecurity technological and industrial capacities in the Union. It would involve the national coordination centres as well as EU institutions and bodies with relevant expertise.

[4] The Competence Centre would enhance synergies between the civil and defence dimensions of cybersecurity in relation to the European Defence Fund by providing advice, sharing its expertise and facilitating collaboration among relevant stakeholders, but also managing multinational cyber defence projects when requested by Member States, and thus acting as a project manager.

[5] This section aims to provide a flavour of the debate and is not intended to be an exhaustive account of all different views on the proposal. Additional information can be found in related publications listed under 'EP supporting analysis'.

DISCLAIMER AND COPYRIGHT

This document is prepared for, and addressed to, the Members and staff of the European Parliament as background material to assist them in their parliamentary work. The content of the document is the sole responsibility of its author(s) and any opinions expressed herein should not be taken to represent an official position of the Parliament.

eprs@ep.europa.eu (contact)

www.eprs.ep.parl.union.eu (intranet)

www.europarl.europa.eu/thinktank (internet)

http://epthinktank.eu (blog)

Fifth edition. The 'EU Legislation in Progress' briefings are updated at key stages throughout the legislative procedure.