Governance Foundations for the European Cybersecurity Community

Afonso Ferreira[1(✉)], Christina von Wintzingerode[2], Dirk Müllmann[2], Abdelmalek Benzekri[3], Pierre-Henri Cros[4], Indra Spiecker gen. Döhmann LL.M[2], and Elvire Prochilo[5]

[1] CNRS, Institut de Recherches en Informatique de Toulouse – IRIT, Toulouse, France
Afonso.ferreira@irit.fr
[2] Goethe-Universität Frankfurt am Main, Frankfurt, Germany
[3] Université Paul Sabatier, Institut de Recherches en Informatique de Toulouse – IRIT, Toulouse, France
[4] Université Paul Sabatier, Toulouse, France
[5] Pragma-Consult, Toulouse, France

Abstract. While Regulation EU 2021/887 of 20 May 2021 established the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres, it has not addressed in any detail the identification, structuring, or coordination of the cybersecurity actors in Europe. This paper proposes their structure and input, extending on work done in the project CyberSec4Europe, which was funded by the European Commission to design, test, and demonstrate potential governance structures for the European Cybersecurity community.

Keywords: Cybersecurity · Community · Governance

1 Introduction

Regulation EU 2021/887 of 20 May 2021 established the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres. With this, the European legislator intends to end the fragmentation of efforts in research and development of cybersecurity products in the EU.

However, in comparison to the rules regarding the establishment, structure and tasks of the European Competence Centre and the national coordination centres, the establishment, governance structure and tasks of what the regulation termed the "Community" are rather vaguely described in the Regulation.

It is against this background that the European Commission decided to fund four pilot projects to help build and strengthen cybersecurity capacities across the EU, as well as provide valuable input for the set-up of the Cybersecurity Competence Network with a European Cybersecurity Research and Competence Centre. These projects are Concordia, CyberSec4Europe, ECHO, and Sparta.

The pilot CyberSec4Europe designed, tested and demonstrated potential governance structures for a future European Cybersecurity Competence Network using best practice examples derived from well-proven concepts like, e.g., CERN (for more examples see [1, pp. 21–33] [2, pp. 4–25, 29–32]), as well the expertise and experience of partners.

With a focus on community-building and thus bottom-up approaches to identify and solve cybersecurity-related problems, the CyberSec4Europe pilot project proposed the installation of additional regional, sectoral and cross-border networks at the Community level. As one element to achieve this goal, CyberSec4Europe envisioned the introduction of Community Hubs of Expertise in Cybersecurity Knowledge (CHECKs) into a future form of the regulation. The network would be significantly strengthened and advanced into a true structure that would ensure efficient flows of information that are implemented swiftly and occur within the most efficient layers.

Accordingly, this paper contributes to the foundations of a framework facilitating the emergence of bottom-up communities of knowledgeable cybersecurity experts that would also integrate potential users and their needs, including from the civil society.

2 Legislative Framework–Regulation (EU) 2021/887

With Regulation (EU) 2021/887 of 20 May 2021[1] the European legislator intends to end the fragmentation of efforts of the industrial and research communities in cybersecurity and to pool and network the existing wealth of expertise and experience in the EU instead.[2] Building sufficient technological and industrial capacities and capabilities shall enable the Union to autonomously secure its economy and critical infrastructures and become a global leader in the area of cybersecurity.[3] For the implementation of these goals the Regulation provides for the interaction of different relevant stakeholders[4] from public entities, Member States and the Union as well as from industry, academia, research and other civil society entities. The Regulation established the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres.

2.1 Categories of Actors

The Regulation divides the different stakeholders into three categories of actors. The European Cybersecurity Competence Centre and its tasks, organisation and funding are the main regulatory object. Its mandate is to support the Union in strengthening capacities and capabilities in all areas of cybersecurity and improve the EU's competitiveness in cybersecurity[5] by pursuing objectives like the promotion of cybersecurity research,

[1] Hereinafter "the Regulation". All Articles and Recitals referred to in this chapter are those of the Regulation, unless explicitly named otherwise.
[2] Recital (7).
[3] Recital (12).
[4] Recital (10).
[5] Art. 3.

innovation and implementation, the creation of capacities, skills, knowledge and infrastructure in this field and the bringing together of stakeholders in a common European cybersecurity ecosystem[6]. Its tasks are divided into strategic and implementation tasks.[7]

As a second category of actors the Regulation provides for the National Coordination Centres and the Network of National Coordination Centres.[8] Their tasks[9] include the provision of expertise, the functioning as a national contact point and the support of the Competence Centre in its assignments. In particular, that includes the coordination and involvement of stakeholders, the improvement of knowledge about cybersecurity in the Member States and the promotion and dissemination of the results of the Network's work.

Finally, the Regulation provides for the Cybersecurity Competence Community.[10] The Community supports the Competence Centre and the Network of National Coordination Centres and shall enhance, share and disseminate cybersecurity expertise across the Union. It shall consists of a broad variety of cybersecurity stakeholders from industry, research, politics and civil society and is thus intended to bring together these key players with other national and European cybersecurity institutions.

2.2 The Cybersecurity Competence Community

The Competence Community is the largest and most diverse group of actors subject to the regulation. Notwithstanding, its establishment, governance structure and tasks are rather vaguely described in comparison to those of the European Competence Centre and the National Coordination Centres. The following analysis focuses on the strengths and weaknesses of this approach in the light of the goals the Regulation is aiming at.

Members and Membership. A community can be characterised as a group of individuals or individual entities with a mutual bond and/or pursuit of common goals (translated definition [3]). The compound term "Competence Community" in the Regulation thus suggests that potential members must not only have a certain affinity, but above all must also have certain competences in the field of cybersecurity.

The broad variety of potential members from industry, including SMEs, academic and research institutions, civil society, European standardisation organisations, public bodies dealing with operational and technical cybersecurity issues, and stakeholders from sectors with an interest in cybersecurity and facing cybersecurity challenges[11] serves the stated objective of bringing together the main stakeholders in the field of cybersecurity in the European Union. However, by whom and according to which criteria the importance is to be determined remains completely open. Due to the lack of normative standards in this regard, it cannot be evaluated at all whether or not the stated goal of bringing together the "most important" stakeholders has been successfully achieved.

[6] Art. 4.
[7] Art. 5.
[8] Rules for their establishment are laid down in Art. 6.
[9] Art. 7.
[10] Art. 8.
[11] Art. 8(2).

Obtaining membership takes place in two steps. First, the National Coordination Centre of the Member State in which the respective institution is established must check whether the institution fulfils the membership criteria. If this is the case, the institution can, in a second step apply for registration as a member of the Community with the European Competence Centre.[12]

The criteria for the membership are a combination of capacity requirements and a catalogue of areas of expertise in the field of cybersecurity. An entity wishing to become a member of the Community must demonstrate that it can contribute to the mission of the Competence Community and has expertise in at least one of the specified areas.[13] The intention to establish a multidisciplinary Competence Community by including as many types of institutions as possible by listing a wide range of areas of cybersecurity expertise becomes very clear from the membership criteria.

The weak point, however, is how possible members who are not already well networked and informed should learn about the possibility of application and registration and, vice versa, how the Community gets to know about new members. Ensuring not only that all possible members get to know about the Competence Community and the possibility of a membership, but also to keep the Community updated on new members will therefore be crucial to establish an agile Community and to exploit its full potential.

Possible Role of the Community. How the Community can contribute to the success of European cybersecurity does not only depend on the recruitment of members but also on the role the Regulation assigns to the Community. The Regulation is very concise when it comes to an explicit description. However, the tasks assigned to the Community as well as its integration into the structure of the European Competence Centre and intended cooperation with the National Coordination Centres and the Network offer valuable clues on that.

Tasks. In the literal sense, a distinction can be made between the Community's own tasks and support tasks. The Community (as a whole) has the broadly described assignment of promoting, sharing and disseminating cybersecurity expertise throughout the Union.[14] The Regulation does not specify, how or by which means this task is to be accomplished. In addition, the Community has a supporting role in fulfilling the missions of the Competence Centre and the Network by involving both in its work[15] and by providing advice through its working groups and the Strategic Advisory Group in the Competence Centre on issues related to the agenda, the annual and multi-annual work programme[16].

The tasks of the members of the Community are laid down separately in Art. 9 of the Regulation. These tasks assign the members a supporting role in the fulfilment of the tasks of the Competence Centre and the Coordination Centres and provide for participation in certain activities and the working groups established by the Governing Board. An independent performance of tasks by the members is only envisaged to a very limited extent. The members' own tasks could only arise indirectly through the Community's

[12] Art. 8(4).
[13] Art. 8(3).
[14] Art. 8(1).
[15] Art. 8(2), e.g., refers to the National Coordination Centres.
[16] Art. 8(9).

tasks regarding the promotion, sharing and dissemination of expertise. Due to the lack of an internal structure of the Community, however, an organised division and execution of these tasks is just as little possible, at least within the framework of the Regulation, as a subsequent self-monitoring with regard to the success or failure of the performance of tasks and possible need for improvement. Thus, the Regulation does not encourage the formation of a Community through the organised joint performance of tasks.

Integration into the organisational structure of the European Competence Centre. Members of the Community may attend meetings of the Governing Board as observers only, without voting rights, at the invitation of the Chairperson of the Governing Board.[17] Permanent observer status is not envisaged for the Community. Neither the Regulation nor the Rules of Procedure of the Governing Board contain any arrangements on the selection criteria for which member(s) of the Community should be invited to a meeting. In this respect, it is important to ensure equal distribution of participation opportunities for representatives of different groups of stakeholders and within these groups. Even if the participating members of the Community do not have voting rights, the position as observer possibly conveys impressions and information that other Community members do not receive at all, only incompletely and/or with delay and which in turn could e.g. be important for their own strategic or economic decisions. Even the appearance of favouring certain members or interest groups needs to be avoided.

In addition to the Governing Board and the Executive Director a Strategic Advisory Group is also part of the permanent structure of the Competence Centre.[18] The selection of members for the Strategic Advisory Group is provided for in the Single Programming Document 2022–2024 of the Governing Board in the period up to and including 2023 [4, p. 14]. This group consists of a maximum of 20 members, which are selected by the Governing Board from among the representatives of the members of the Competence Community upon the proposal of the Executive Director.[19] The Competence Community itself is neither involved in the proposal nor the selection process. Thus, the Strategic Advisory Group is explicitly not a representation of the members of the Community to the Competence Centre in the sense of democratic participation. At least the rules on the composition of the group are intended to ensure a balanced reflection of the Community.[20] Nevertheless, the procedural rules for appointing the members of the Advisory Group[21] [5] still show room for improvement. For example, there are no rules for the case that more than 20 equally suitable member representatives respond to the call of the Executive Director and whether or how extensively the decision for the selection of the listed members would have to be justified and published. It must also be ensured that the call is made equally accessible to all members of the Competence Community.

[17] Artt. 12(6), 14(5).
[18] Art. 11(2)(c).
[19] Art. 18(1)(2).
[20] Cf. Art. 18(1).
[21] Art. 18(3) Regulation i.c.w. Art. 20 of the Rules of Procedure of the Governing Board.

The mode of operation of the Advisory Group is only roughly determined in the Regulation.[22] Once established, the Advisory Group shall adopt its own rules of procedure.[23] As its name suggests, the Strategic Advisory Group has only an advisory-supporting role in the Competence Centre[24]. It may e.g., decide on and organise public consultations, but these require the approval of the Governing Board.[25] The Governing Board may, but is not obliged to, invite a representative of the Advisory Group to its meetings.[26] The Advisory Group, unlike ENISA,[27] does not have a permanent observer status on the Governing Board and the Group members have thus no obligatory right to attend the Governing Board meetings. They have also no voting rights in Board decisions. Furthermore, the Governing Board does not have to follow the recommendations of the Strategic Advisory Group, nor does it have to justify or at least give reasons for deviations.[28] Overall, the degree of participation of the Advisory Group in the work and decisions of the Board is remarkably weak.

Despite that, it is still to be welcomed that the Council's position in the legislative process to not integrate a body of the Competence Community into the structure of the Competence Centre at all was ultimately not able to prevail[29]. The Strategic Advisory Group is at least one permanent point of contact between the Competence Centre and the Community. However, with the decision not to design the Strategic Advisory Group as a representation of the Competence Community and to create very limited opportunities for its participation, an opportunity was missed,[30] [6, p. 483] [7, p. 693] to create a real incentive not only for the participation in the Advisory Group, but also for a membership in the Competence Community in general.

Another field of activity for the members of the Community are working groups, established by the Governing Board under consideration of the recommendations of the Strategic Advisory Group.[31] Where necessary, the coordination of the working groups is carried out by one or more members of the Strategic Advisory Group.[32]

22 The Governing Board has so far only made a provision in Art. 20 of its Rules of Procedure for the appointment procedure, but has not defined and published the working methods of the Strategic Advisory Group. It is quite conceivable that the rules of procedure will be supplemented after the advisory group has been established.

23 Art. 19(5).

24 Cf. Art. 20.

25 Art. 20(c).

26 Art. 12(7).

27 Unlike ENISA, the Strategic Advisory Group is not a permanent observer in the meetings of the Governing Board, cf. Art. 12(7).

28 Neither does the Regulation provide for a duty to state reasons, nor is there a voluntary commitment by the Governing Board in its Rules of Procedure.

29 Council of the European Union, Mandate for negotiations with the European Parliament, 9 March 2020, proposal and remark 27, Interinstitutional file 2018/0328(COD), Doc. No. 7616/19, 26.03.2019.

30 The criticism towards the limited role of the Scientific-Technical Advisory Board in the analysis of the Regulation Proposal is in this respect transferable almost unchanged to the Strategic Advisory Group.

31 Art. 13(3)(n) i.c.w. Artt. 8(9), 9(b).

32 Art. 19(2).

Unlike the Strategic Advisory Group, the working groups are not permanent structural elements in the Competence Centre with specific tasks of their own. Specific working groups can be set up to collaborate on issues relevant to the work of the Competence Centre[33] and to provide advice on the agenda, the annual and multi-annual work programme[34]. This is a quite narrowly defined assignment of tasks on a case-by-case basis by the Governing Board to individual members of the Community. Unfortunately, neither the Regulation nor the Rules of Procedure of the Governing Board[35] provide for procedural rules or criteria for the selection of these Community members. Such rules would be desirable not only from a rule of law perspective, but also for community building. Ensuring a certain plurality and diversity of the working groups can indirectly lead to new contacts and exchange between Community members, who are not already networked. This, in particular, would promote the dissemination of expertise and could give rise to new impulses for research and development.

Cooperation with the National Coordination Centres and the Network. The Regulation assigns tasks to the National Coordination Centres and the Network, among others, related to the Community and its members.[36] The Network, like the Competence Centre, shall cooperate with the Community as appropriate.[37] The National Coordination Centres shall serve as main contact points for the Community at national level and shall assist the Competence Centre in particular in coordinating the Community through coordination of its members.[38] The promotion and dissemination of relevant work results of the Network, the Community and the Competence Centre at national, regional or local level is also one of the tasks of the National Coordination Centres.[39] It also has to promote, facilitate and encourage the participation of civil society, industry, in particular start-ups and SMEs, academia and research and other stakeholders in cross-border projects and cybersecurity activities at national level.[40] While this task is in fact not directly related to the Community, it does also not explicitly exclude its members. In addition, National Coordination Centres can help stimulate interest in a membership and encourage appropriate institutions to join the Competence Community.

In return, the Community shall e.g., involve the National Coordination Centres in its work[41]. Its members shall work closely with the National Coordination Centres to

33 Cf. Wording in Art. 19(2).

34 Cf. Wording in Art. 8(9).

35 Art. 14 of the Rules of Procedure of the Governing Board deals with "working groups", but the Regulation does not refer to the working groups in the Regulation. In terms of content, it deals with "*ad hoc* working groups", the necessity, formation and composition of which seem to be conceived differently from the working groups mentioned in the Regulation. A clearer description in the Rules of Procedure (and, if necessary, a definition of the terms) would be desirable.

36 Cf. Art. 7(1).

37 Art. 3(2).

38 Art. 7(1)(a).

39 Art. 7(1)(h).

40 Art. 7(1)(c).

41 Art. 8(2).

assist the Competence Centre in fulfilling its mission[42] and shall assist the National Coordination Centres in promoting specific projects[43].

Opportunities and Barriers for Community Building. The Regulation, thus, creates possible touching points between the Coordination Centres as public actors and the Community or its members as predominantly private law actors. The role of the National Coordination Centres "in the middle of the action" offers a suitable starting point for the creation of national, regional or local communities and networking within the Community, if designed actively and purposefully. The complementary mandate for the Community to work closely with the Coordination Centres supports this approach. However, the Regulation does not lay down structures for practical task implementation and cooperation. Thus, it is left to the National Coordination Centres and the Competence Community to design these. The resulting freedom of design offers both sides the opportunity to take national, regional or local, thematic and sector-specific circumstances into account for the cooperation design. A realistic approach must of course still be aware of the danger that the individual efforts in the Member States fail and that no cooperation at all or no sufficient cooperation for the promotion of European cybersecurity is achieved. While the National Coordination Centres, as public institutions, have an internal structure "by order" and can use traditional forms of action under their national legal systems, the *Competence Community,* contrary to its name, is not yet a structured unit that can revert to such common organisational or financial resources. Whether and how the cooperation will succeed in practice therefore remains to be seen.[44] [1, 2, 8].

Considering that the Competence Community - despite or precisely because of the thematic affinity of its members - will include competitors with opposing interests, e.g. with regard to political influence, funding opportunities or expansion of market shares, an "automatic" or "natural" formation of a Community seems far-fetched. Although the Regulation lays down the criteria and procedure for becoming a member of the Community, it does not contain any explicit rules on how to build the Community from the registered members and which structures it can actively use to fulfil its tasks. Thus, the tasks of the Community and its members as well as their integration into the governance structure of the Regulation, can give at most only clues as to what kind of Community the legislator had in mind. As demonstrated, however, the Regulation alone does not contain powerful enough community-forming factors.

The broadly chosen community concept is the best approach to cover as many areas and existing competences in the field of cybersecurity in the European Union as possible. Another question, however, is whether the broad notion of a Community in theory can be brought to practical life at all. The participation design is one decisive element in this regard. Studies on private standardisation organisations, which could also be described as communities, demonstrate that regularly only those stakeholders with the necessary

[42] Art. 9(a).

[43] Art. 9(c).

[44] According to Recital (17), with regard to the management of the Community and its representation in the Competence Centre, e.g. the experience of the 4 pilot projects CONCORDIA, ECHO, SPARTA and CyberSec4Europe, which were launched at the beginning of 2019 within the framework of Horizon 2020, shall be drawn upon. CyberSec4Europe has extensively addressed governance design issues for the Competence Community.

financial, time, and human resources can exert active influence, because this is what makes active participation possible in the first place. Not all interests therefore have the same chances of assertion [9, p. 174], even if in principle everyone can participate [9, p. 117] [10, p. 38 et seqq.]. The resulting work therefore only reflects the contributions of the actively involved, assertive stakeholders and is not a consensus of all stakeholders. This effect cannot be ruled out for the Competence Community. The organisational efforts that come with an involvement of Community members within Community networks, in working groups or in the Strategic Advisory Group may exceed the organisational possibilities of smaller members, no matter how much expertise and experience they have. Particularly in the field of cybersecurity, with rapid technical developments and effects that reach into every area of society and government, it is undesirable to leave existing competences unused only due to structural deficits of the participation design in the Regulation.

3 Organising the Community

As discussed above, it is essential to activate and effectively use the potential that lies within the concept of a Competence Community. The Regulation's top-down approach and the limitation of Community members to observing or advisory roles without real opportunities for influence do not offer much incentive for an active involvement, while the exclusive participation design makes it even more difficult to exploit existing competences. Opportunities for the cooperation, collaboration and knowledge exchange within the Community as well as funding opportunities for its members have to be ensured in order to reach this goal.

Therefore, the fact that the Regulation does not offer sufficient instruments for the establishment and governance of the Community should be seen as an opportunity. The absence of strict rules leaves space for the development of a true bottom-up approach for the Community building. The power of bottom-up approaches results from their possibility to provide broad expertise and knowledge of industry, academia and stakeholders in specific areas by organising information gathering and distribution. It is, thus, an appropriate way of activating research and development capacities.

One way to establish and organise the Community could therefore be the introduction of hubs in which different stakeholders could join their efforts, accumulate special expertise, promote scientific exchange and facilitate research or development of solutions. These Community Hubs of Expertise in Cybersecurity Knowledge (CHECKs) would be low-level, easy-to-access points of accumulation of regional, sectoral or topical interests and information, and they can serve as accelerator to demands and problem identification as well as solution mechanisms.

We note that CHECKs are different from the Digital Innovation Hubs (DIHs) launched by the European Commission in fundamental ways. DIHs were launched by European Commission in the scope of the Digitising European Industry initiative in 2016, in order to coordinate with Member States and regions towards common goals to help companies to become more competitive with regard to their business/production processes, products or services using digital technologies. In the new programme Digital Europe (2021–2027), they are called European DIHs (EDIHs) and defined as one-stop

shops supporting companies to respond to digital challenges and become more competitive. They provide access to the latest knowledge, expertise and technology to support their customers with piloting, testing and experimenting with digital innovations [11, 12].

As a first step it is necessary to further develop the idea of CHECKs. Their optimal design requires answering a variety of questions, such as the organisation, composition, tasks and funding of CHECKs as well as their relationship to each other, to the national coordination centres and the European Competence Centre. The answers should be based on practical experience gained in the pilot projects, analysis of legal frameworks, expediency and teleological considerations, and stakeholder feedback [13, 14].

Therefore, the CyberSec4Europe pilot project proposed the installation of additional regional and cross-border networks at the Community level [1, 2, 8]. As one element to achieve this goal, CyberSec4Europe envisioned the introduction of CHECKs into a future form of the regulation. The network would be significantly strengthened and advanced into a true structure that would ensure efficient flows of information that are implemented swiftly and occur within the most efficient layers. It has to be noted that also from the point of the Community membership it can be advisable to establish different decision-making processes, which will not always include all partners on all issues.

3.1 Our Use-Case

Two types of CHECK emerged after the preliminary analyses, namely one that is an economic actor in the cybersecurity landscape and must be sustained by a sound business model, and another that is part of the public administration and financed as a public good. The case described here, namely the CHECK-T pilot, in Toulouse, France, that is used to validate a specific governance model, is an example of the former type.

In view of the implementation of CHECK-T, interviews were conducted with stakeholders in order to learn about their needs and requirements regarding CHECKs, e.g., which details make the concept of CHECKs attractive for them to participate and contribute to the cybersecurity Community. These results together with possible changes in the governance structures may constitute the basis for the improvement of the European cybersecurity governance in future revisions of the regulation.

The interview campaign was carried on in order to identify the main needs and expectations, types of financially sustainable activities and a multidisciplinary pool of actors that would be willing to participate in the creation and development of the CHECK-T, aiming at:

- Mobilise communities of actors with different but complementary challenges
- Project a common vision
- Identify a consensus on the expected missions within the consortium

Highlight the benefits for each stakeholder by sharing, contributing, and financing in common.

3.2 Needs and Expectations

The interview campaign included a total of 40 stakeholders from four large community groups (cybersecurity end users, cybersecurity solutions providers, technology centres,

and economic development accelerators). The expressed needs and expectations were divided in six main categories, as follows.

Capacity building: Guarantee the sharing of data, sensitive information, and technological research with other partners on all types of incidents and on the responses provided.
Transfer of uses, sharing of R&D&I costs: implementing methodological processes transferable from one sector to another, at lower costs.
Technological leadership: Sharing expertise and general know-how, infrastructure, and investment costs by obtaining R&D funding.
Trust-building: Building a local and European base of trust, promoting cooperation and coopetition between members (ethical framework, protection of freedoms, dissemination of trust).
Business Return On Investment (ROI): facilitate the obtaining of funding in Cybersecurity Innovation and accelerate the maturation of projects and products to the market and awareness-raising, co-innovation activities.
Usability by design: Eliminate barriers by studying use cases and demonstrating scientific and technological know-how before large-scale deployment towards industrial products.

Such analysis is summarised as follows.

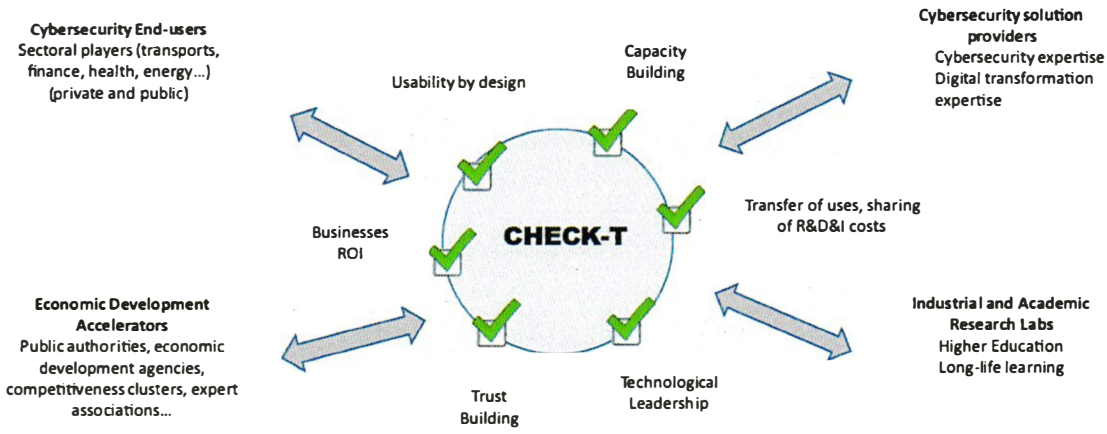

Fig. 1. Community groups and mission classes for a CHECK

3.3 Main Findings

In each of the six categories described above, possible interactions between the actors (from one community group to another and peer-to-peer by highlighting the concept of coopetition) were further explored. Some remarkable examples by category include:

Capacity building: Information sharing, including common interpretation of cybersecurity legal texts.
Transfer of uses, sharing of R&D&I costs: Here again information sharing was central, e.g. about best practices.

Technological leadership: Pooling of lobbying activities.
Trust-building: Agreeing and publishing a common ethical framework of cooperation.
Business Return On Investment (ROI): Very important point, that includes networking, market access, and the identification of funding opportunities.
Usability by design: Elicitation of requirements that may be common to many members.

A comprehensive synthesis of the main findings is given in the figure below.

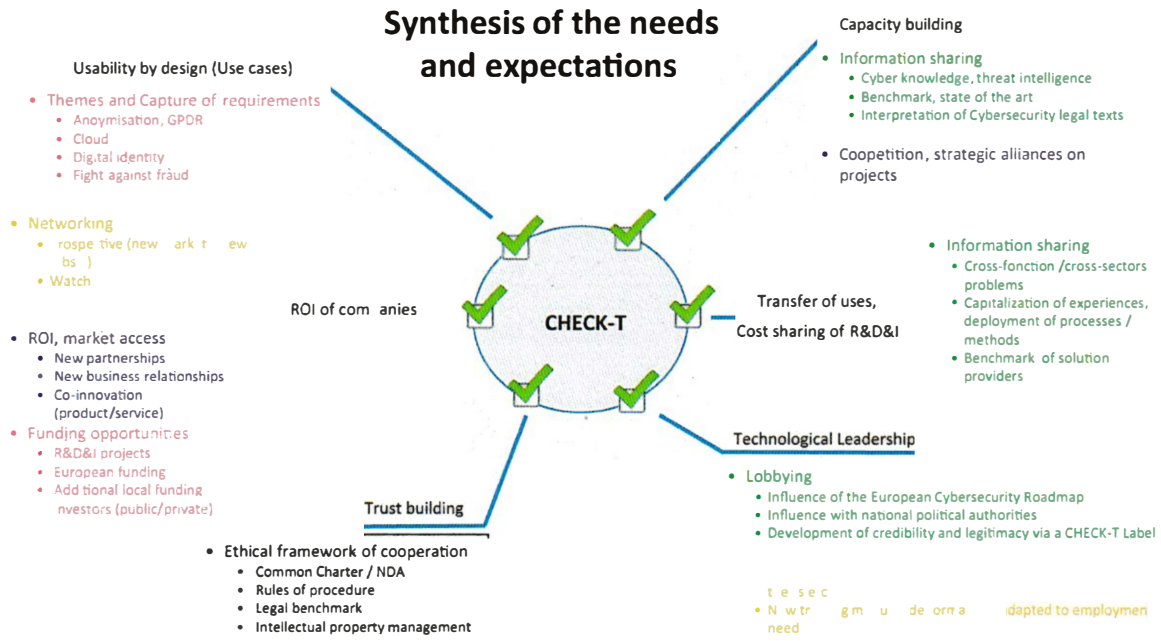

Fig. 2. Synthesis of the needs and expectations

The next step defined four strategic application areas, which must be implemented in order for the stakeholders to take an interest in the creation of a CHECK:

R&D&I funding
Services
Market access
Skills upgrade

In each of these areas, several priority and evolving activities have been identified and are described below.

Finally, the following activities emerged as foundational in order to increase the likelihood of success of a CHECK.

R&D&I funding: Exploration of the opportunities to participate in European and national calls for projects in AI and cybersecurity.
Services: Networking and lobbying in order to influence cybersecurity roadmaps, e.g. within the CyberSec4Europe project.
Market access: Fight against banking fraud as a first use-case, based on the decompartmentalization of business data.

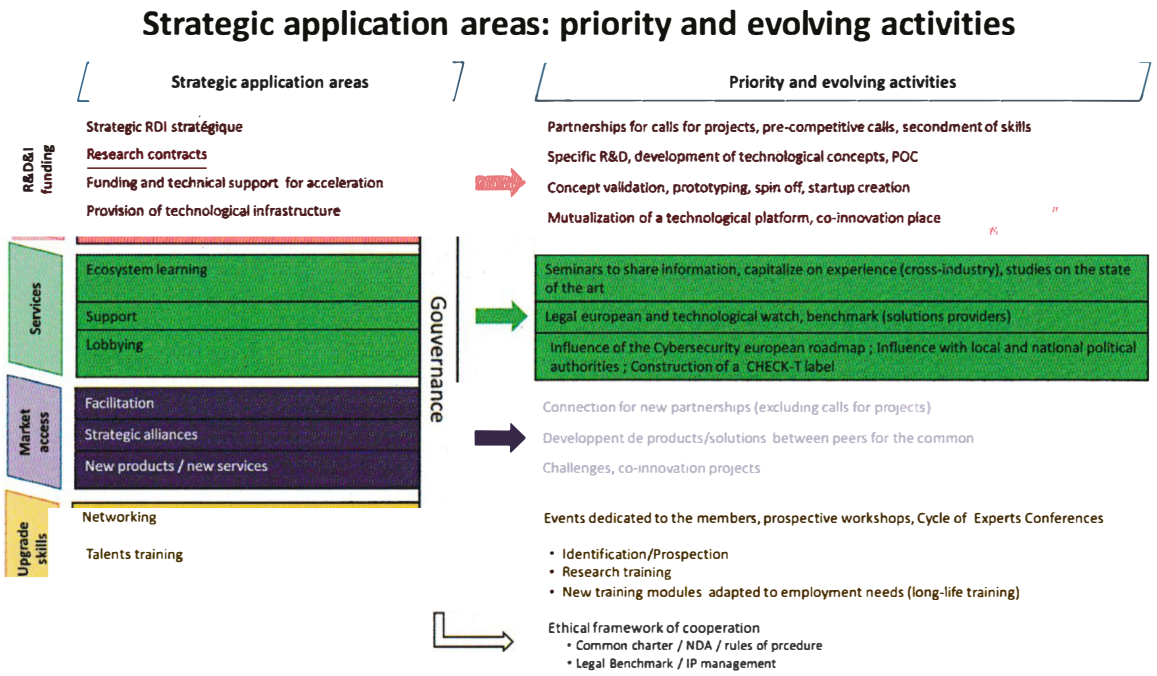

Fig. 3. The four strategic application areas emerging from the interview campaign

Skills upgrade: Development of a training catalogue, based on skill blocks, especially in what concerns AI and cybersecurity.

Giving priority to such activities would provide CHECKs with clear milestones to guide the start of their implementation. Among them, one particular task stood out as a common ground underpinning these different activities, namely answering calls for proposals, which can be explained by their expected and tangible returns on investment. As a consequence, this common feature was chosen as a first working basis for defining the financial value that CHECKs should have, in order to bring its potential members to join and work towards effectively implementing and developing the above four activities.

Following this line of reasoning, a CHECK may propose itself as a tool for its members to target regional, national, and European calls for proposals, for instance by selecting specific calls for proposals and then identifying and coordinating its competent members that are best fit for answering them. In such a case, CHECKs' role would be either to build and coordinate appropriate skills consortia to respond to calls for projects, or to identify and orchestrate the available skills necessary to join, as a partner, larger consortia preparing to respond to calls for projects. This could also be done by considering that the CHECK, as the representative of the community of competence of its territory, would be the legal entity participating in the response submitted to the call, on behalf of its subset of selected members.

Both the coordination of proposals and the participation in consortia imply that a CHECK must be in possession of a complete and up-to-date inventory of the skills and the knowledge available among its members in the field of cybersecurity, and be informed of their availability and intention to participate in the implementation of such collaborative projects.

4 Recommendations

The analysis carried out reveals potential for improving the role of the Community in various areas. For a successful exploitation of the existing knowledge and expertise of the Community, the current regulation lacks instruments and incentives for their involvement, and this has to be overcome. In this section we give recommendations pertaining to these aspects, in order to remediate missing features of the regulation. Legal as well as organizational and financial aspects have to be taken into account.

4.1 The Review of the Cybersecurity Regulation

A revision of the regulation by the European legislator should consider at minima the following points.

Potential Community members or already existing networks need to be approached systematically to inform them about the possibility of application and registration and, even more important, about the benefits and added values of a membership in the Community. It needs to be clear why a stakeholder should decide to apply for the Community and put efforts into the tasks that come with a membership.

The participation of Community members should be strengthened, e.g. in the Strategic Advisory Group. The Group should be given a permanent observer status in the meetings of the Governing Board and the Board should be obliged to give an explanatory statement in case of full or partial non-consideration of advice given by the Strategic Advisory Group. It should also be considered to give the Community a voice in the decision which of its members join the Strategic Advisory Group. Participation and representation in decision-making processes are benefits that should not be underestimated.

The Community needs a governance structure, which allows for an organised approach on the existing cybersecurity challenges while offering the necessary flexibility as an answer to the diversity of stakeholders and circumstances in the Member States.

More obvious, but not less important than participatory or organisation instruments, is the dedication of funds to certain tasks or projects to encourage research and development activities in the Community. This can either encourage the collaboration of members in already existing connections as well as the establishment of new ones, e.g. for specific tasks.

4.2 Governance of CHECKs

As indicated above, governance issues are transversal to the strategic application areas and depend on the specific activities to be implemented. The appropriate governance model to be chosen depends a great deal on decisions needed to implement the inventory described above, as it can be considered the capital on which a CHECK must be based. In order to carry out such an inventory as efficiently and comprehensively as possible, it is necessary to quickly determine the group that will participate in the foundation of the CHECK, i.e. whether or not it will be composed only by representatives from the End User, Cyber Security Solution Providers, Technology Centres, and Economic Development Accelerators communities that have been consulted in order to define the strategic axes and the priority activities.

Accordingly, the first decision of the group of founders should be to agree on the subject matter of CHECK, and therefore its role, in particular with respect to the calls for proposals. This is because both subject and role would delimit the appropriate legal status that is required for a CHECK to become a legal entity. The choice of a legal status will also help to determine the contractual nature of the inventory, which may be a simple directory of territorial competences in the area or a database of relevant persons, staff or not, from the communities that constitute the CHECK, and on which it will rely to participate in calls for proposals and to fulfil its contractual commitments once the project is implemented. It is worth noticing that one of the main added-values of a CHECK to the current cybersecurity regional landscape in the EU is exactly this capacity to coordinate and orchestrate exogenous and diverse skill resources in the form of a cooperative with a legal status.

Therefore, the governance model should be discussed by the founders of CHECKs in order to establish an internal organisation that is conducive of the role to be implemented, but, crucially, cannot create competition to their own members. This last point needs particular attention, as it directly impacts the economic model of a CHECK, as discussed in the following.

4.3 Funding and Sustainability

The abstract concept of a CHECK is very attractive and all interviewed stakeholders were very positive about its priorities, membership, activities, and so forth. However, questioning starts immediately once aspects related to the funding of such activities come to fore, as very few stakeholders are eager to embark in such a journey if they are not first shown how their financial investment would enable the generation of income for themselves and in a near future, through such activities. This is why the orchestration of skill resources emerged as a priority task for a CHECK, as it makes CHECKs primarily a source of revenue for its members, which may then be complemented with activities around lobbying, sharing good-practices and information, and capacity building.

In this sense, if a CHECK is established as a cooperative means for its members to target regional, national, and European calls for proposals, and to coordinate the corresponding responses, then funding should normally be implemented through a mix of (i) membership fees paid by its constituting members, (ii) access fees for consultation of its directory, (iii) consultancy fees related to the facilitation of participation in calls for proposals, as well as through (iv) bonus schemes on the results.

We note that if the decision is to establish the CHECK as the legal entity that is to be contracted in successful responses to calls of proposals, on behalf of its members, then the funding would also include the collection of overheads and administrative budget of projects won. On the other hand, such a decision should be dependent on the satisfactory resolution *ex-ante* of thorny IPR issues. As a matter of fact, this should not be considered as an impediment, since very successful examples of this kind of organisation exist, notably IMEC in Belgium.

Another important point of attention for CHECKs as legal entities is the fact that calls for proposals usually come with stringent rules on the financial capacity of bidders. Therefore, a CHECK bidding in calls for proposals should be able to demonstrate that the amounts for which it bids represent a fraction of its financial capacity, which is given

by its capital and turnover. It is likely that the amount of equity allocated to a CHECK will be the result of the discussions with the founders as it will reflect the level of their ambition. The turnover could be based on the combination of the membership, access, and consultancy fees and bonuses alluded above.

As a result, in order to quickly ensure the feasibility and relevance of the approach chosen for a territory, it is recommended to go through a phase where the formal "pre-configuring" of the organisation to be established is funded. Its effective implementation implies favouring legal support by an actor in the territory with a certain notoriety in the targeted ecosystem. By thus incubating a CHECK, such an actor would enable the CHECK to attract funds to deploy a first structuring project prototype that would demonstrate the robustness and sustainability of its economic model, whereby kickstarting the legitimacy and the added-value of the CHECK in the eyes of its stakeholders.

Finally, as part of such a partnership logic, this model based on a seed legal support by a third party should favour a structure with mainly public capital. Indeed, the production of common deliverables by a multidisciplinary ecosystem requires an environment of trust from the outset that only public authorities can guarantee at that point.

5 Conclusion

The case of the CHECK-T pilot that was tested by CyberSec4Europe, through its partner UPS-IRIT, contributed notable insights based on day-to-day implementation experiences, including the existence of some mistrust from the part of public administrations themselves, because of issues related to their perimeter of action and influence.

In view of the installation of additional European regional and cross-border networks at the Community level, CyberSec4Europe already envisioned the introduction of CHECKs into a future form of the Regulation while the legislative procedure was still in progress. Unfortunately, this has not been considered by the legislator and if it will be considered in case of an amendment, cannot be foreseen. However, despite the missing support of the CHECK concept, there are at least no limitations in the Regulation for the Community to organise itself.

For stakeholders to take an interest in CHECKs, four strategic application areas must be implemented, namely access to funding in R&D&I, capacity building, market access, and dedicated services. Such services to be offered could then contribute to the economic security of the so-called essential sectors of the territory and would have as primary vocation to support the rise in the capacities of SMEs / SMIs and subcontractors of these sectors, in their approach to crisis management, in particular related to cybersecurity. The development and deployment of services related to the establishment of a CHECK would be done in close partnership with solution providers and the research and higher education communities in the region.

Finally, Member States and, wherever necessary, their regions, should provide dedicated funds to kick-start contractual Public-Private partnerships with the CHECKs in order to increase their attractivity in the eyes of stakeholders. As described in this paper, our interview campaign elicited the needs from potential stakeholders and highlighted services expected from such an organisation. The needs and potential services detailed here are meant to serve as a basis upon which to build the CHECKs' business models in

future. Public seed-funds are crucial in that they would help to create a virtuous circle, where the return-on-investment in joining one such CHECK becomes more evident.

Acknowledgments. This work was based on very rich conversations with the members of Work Package 2 of CyberSec4Security, whom the authors warmly thank. This work was partially supported by the European research projects H2020 CyberSec4Europe (GA 830929) and LeADS (GA 956562) and Horizon Europe DUCA (GA 101086308), and by the CNRS IRN EU-CHECK.

References

1. CyberSec4Europe H2020 Project. D2.1 Governance Structure (2020)
2. CyberSec4Europe H2020 Project. Deliverable D2.3: Governance Structure v2.0 (2021)
3. Duden online. https://www.duden.de/Rechtschreibung/Gemeinschaft. Accessed 25 Oct 2022
4. European Cybersecurity Competence Centre. https://cybersecurity-centre.europa.eu/system/files/2022-08/GB%20decision%20No%202022_6_ECCC%20SPD%202022-2024_Budget%202022.pdf. Accessed 25 Oct 2022
5. European Cybersecurity Competence Centre. https://cybersecurity-centre.europa.eu/system/files/2021-11/ECCC%20Decision%20No%20GB20211%20RoP_final.pdf. Accessed 25 Oct 2022
6. von Wintzingerode, C., Müllmann, D.: Ein europäisches Netzwerk für Cybersicherheit, in Den Wandel begleiten - IT-rechtliche Herausforderungen der Digitalisierung, Edewecht, pp. 475–492 (2020).
7. von Wintzingerode, C.G., Müllmann, D., Spiecker gen. Döhmann, I.: Ein Netzwerk für Europas Cybersicherheit, Neue Zeitschrift für Verwaltungsrecht (NVwZ), pp. 690–695, 2021
8. CyberSec4Europe H2020 Project, Deliverable D2.2: Internal Validation of Governance Structure, 2021
9. Bolenz, E.: Technische Normung zwischen "Markt" und "Staat" Bielefeld (1987)
10. Hartlieb, B., Hövel, A., Müller, N.: Normung und Standardisierung, Berlin (2016)
11. Foray, D., et al.: Guide on Research and Innovation Strategies for Smart Specialisation
12. Digital Innovation Hubs, European Commisison. https://s3platform.jrc.ec.europa.eu/digital-innovation-hubs. Accessed July 2022
13. Nai-Fovino, I., Neisse, R., Lazari, A., Ruzzante, G.: European Cybersecurity Centre of Expertise - Cybersecurity Competence Survey. Publications Office of the European Union, Luxembourg (2018)
14. Penchev, G., Shalamanov, V.: Architecture and Process Oriented Approach to Institution. Inf. Secur. Int. J. **46**, 99–113 (2020)