Information & Security

G. Penchev & A. Shalamanova
vol. 46, no. 1 (2020): 99-113
https://doi.org/10.11610/isij.4607

Published since 1998

ISSN 0861-5160 (print), ISSN 1314-2119 (online)

Research Article

A Governance Model for an EU Cyber Security Collaborative Network – ECSCON

Georgi Penchev [a,b] (✉), ***Antoniya Shalamanova*** [c]

[a] *Department "National and Regional Security," University of National and World Economy, Sofia, Bulgaria, https://www.unwe.bg/en/*

[b] *Institute of Information and Communication Technologies, Bulgarian Academy of Sciences, Sofia, Bulgaria, http://www.iict.bas.bg/EN*

[c] *Sofia Development Association, Bulgaria, https://www.sofia-da.eu*

ABSTRACT:

This white paper on governance of European Cyber Security Collaborative Network (ECSCON) is proposed as a joint effort between the four pilot projects ECHO, SPARTA, CONCORDIA and CyberSec4Europe to identify the "umbrella" model for effective and efficient coordination of the development of the European cyber security competence community in the institutional framework established by a European cybersecurity hub with a network of cybersecurity competence centres and in relation to EC, EUMS, ENISA, EDA, EUROPOL, and the NATO Cyber Organization. The white paper combines findings from bottom-up research in CyberSec4Europe and SPARTA with the top-down approach implemented by ECHO and will seek further cooperation with ECSO and Cyber Atlas to achieve a common proposal to the EC and offer to the European cyber security competence community to be self-organized on regional and functional principle. The proposed governance model defines the CNO as a Virtual organisations Breeding Environment to support the establishment of service groups to address specific demand, maintaining a regional (chapter based) organization of the community with a central hub dealing with EC and chapters dealing with the hub and national coordination centres in the respective member-states.

ARTICLE INFO:

RECEIVED: 22 JUN 2020
REVISED: 29 JUL 2020
ONLINE: 31 AUG 2020

KEYWORDS:

Cyber security community, Governance, Collaborative Network Organization, Virtual Breeding Environment, Innovation Management

✉ Corresponding Author: E-mail: gpenchev@e-dnrs.org

Introduction

The specific topic of the implementation of the Regulation of the European Parliament and the Council, establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres [1] (R630) is governance and management of the Cyber Community in Europe. While discussing the findings of the four pilot projects (CONCORDIA, ECHO, SPARTA and CyberSec4Europe), established to assist EU in pooling Europe's cybersecurity expertise and preparing the European cybersecurity landscape in order to efficiently implement the vision for a more secure digital Europe, we discussed to jointly develop a White paper on Governance of the EU Cyber Security Collaborative Network – ECSCON. These projects are assisting the EU in defining, testing and establishing the governance model of a European Cybersecurity Competence Network of cybersecurity centres of excellence[2] in cooperation with ECSO and Cyber Atlas (JRC).

The EU cyber security environment as presented in the Regulation on establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres is presented in Figure 1.

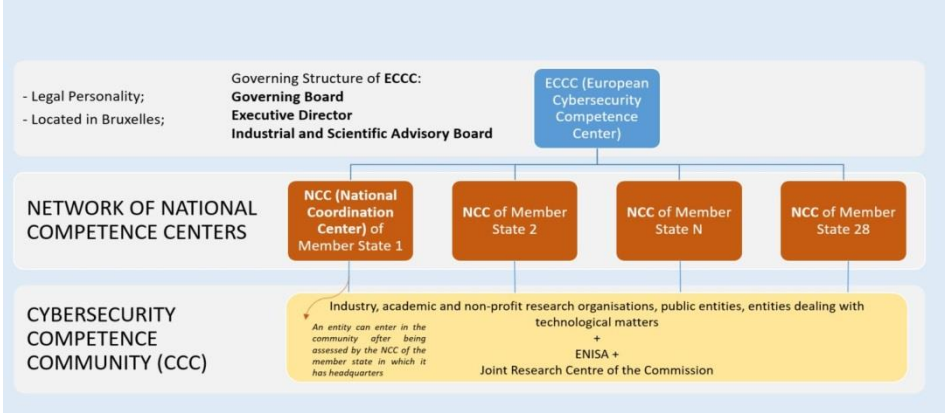

Figure 1: European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres with a Cybersecurity Competence Community.

In regards to the Cybersecurity Competence Community (CCC) we consider establishment of different networks – one definitely is around ECSO, another is developed under Cyber Atlas initiative of JRC, and the four pilots also aim at building their collaborative networked organisations.

The aim of this paper is to present in brief the process of analysis of the governance model alternatives of ECHO Project. It also presents the decision to form an "umbrella" organization which will allow establishment of Virtual Organizations with different governance objectives (services or products) under

the umbrella of one central hub. The flexibility of this type of model enables the opportunity to form a wider European Cyber Security Collaborative Network – ECSON.

Virtual Organisations Breeding Environment (VBE)

VBEs can be described as forms for flexible establishment and restructuring of Collaborative Networked Organisations (CNOs) and considered as possible form of service focus groups. The CNOs can be distinguished by their time horizon, level of trust, consensus and commitment.[3,4]

The ECHO Deliverable D3.1: "Governance needs and objectives", provides in-depth analysis of the literature related to CNOs. One of the useful definitions given in D3.1 about VBE, based on the book by Camarinha-Matos, Afsarmanesh, and Ollus "Methods and Tools for Collaborative Networked Organizations", is the following: [5]

> *A VBE is defined as an association of organisations and related supporting institutions adhering to a base long-term cooperation agreement, and adopting common operating principles and infrastructures, with the main goal of increasing both their chances and preparedness towards collaboration in potential VOs. Establishing trust relationships among VBE members and the ability to assess the trustworthiness of others in the VBE are the basic requirements for the effective operation of VBEs and the creation of successful VOs.*

The umbrella organisation of the VBE, with option for structuring and restructuring itself with establishment, changing and closing its VOs will have specific procedure. A simplified procedure is given in Figure 2.

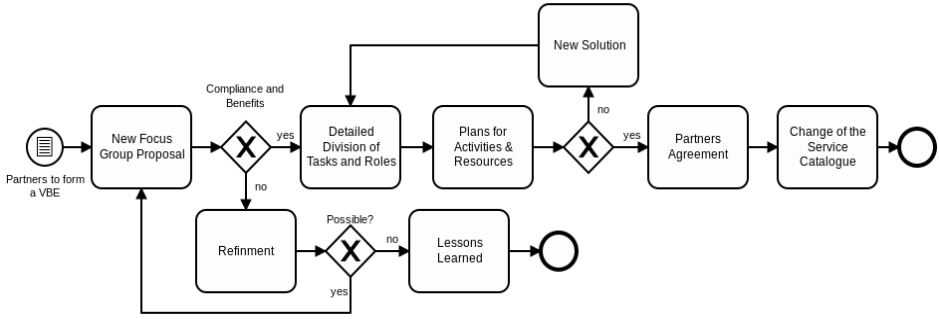

Figure 2: Simplified procedure for new focus group establishment.

This procedure does not consider the actors involved in the process. Figure 3 presents a possible involvement of actors and their activities.

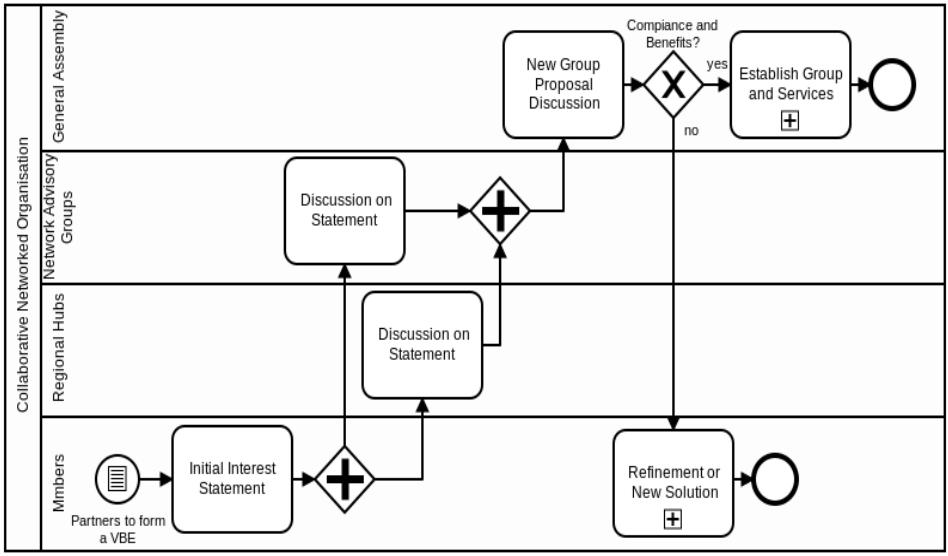

Figure 3: Activities and actors.

The comparison of Figure 2 and Figure 3 shows that such a procedure will have certain points of identification in CNOs' documents. (The two parts of possible process flows after the first decision in Figure 1 are given as sub-processes in Figure 3.)

An "umbrella" governance model

This section provides the context of the ECHO Project goals, tasks and activities related to the analysis and development of a Governance model for the future ECHO CNO, that will be the successor of the current project consortium. The section also describes the prerequisites for the successful ECSCON establishment.

ECHO Governance and Management methodology research framework (developed within activities of project's Task 3.3) from the very beginning was to generate alternatives, based on the mandate (Mission, Vision, Value proposition, and Strategy) for the ECHO organisation. The study on the alternatives uses as input the identified in Deliverable 3.1 needs and objectives to the governance (management) model of the organisation.

After the process of development, assessment, comparison, and sensitivity analysis of the four alternatives, a decision was taken to select none of the presented alternatives, but to develop (see Figure 4) an "umbrella" alternative (A0), combining the common elements of Alternatives from 1 to 4, over and above specific arrangements. This "umbrella" alternative has to be able to address the following issues:

- provide a framework for the "breeding environment";
- generate "partnerships" under more specific predefined models (A1-A4 modifications);
- address certain functional area or sector; and
- provide specific arrangements for multisector or multifunctional solutions to be developed as a capability and offered as a service.

The results from the analysis were presented and the decision was taken during the Workshop on Governance Model Alternatives Assessment and Selection, 12 May 2020, held on-line, where ECSO and other pilot projects participants were invited.

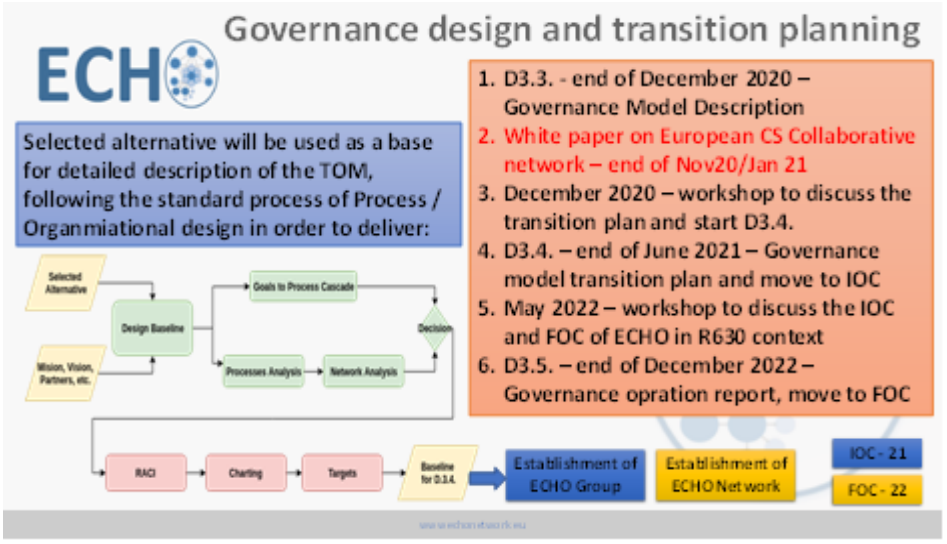

Figure 4: Process of development of Governance model design in ECHO, with opportunity to extend it for the joint development of the Governance model for ECSCON.

The decision to develop "an umbrella" alternative (Alternative 0 – A0) taken during the Workshop on 12th May was followed by some internal ECHO meetings where it was further discussed. It was decided that A0 should provide high-level governance of ECHO Network through a central hub (ECHO Group) with identified core processes, structures, and "umbrella" services in the area of Governance and Management Consulting, Multi-sector Analysis Framework (MSAF) applications and Cyber Skills Education and Training framework.

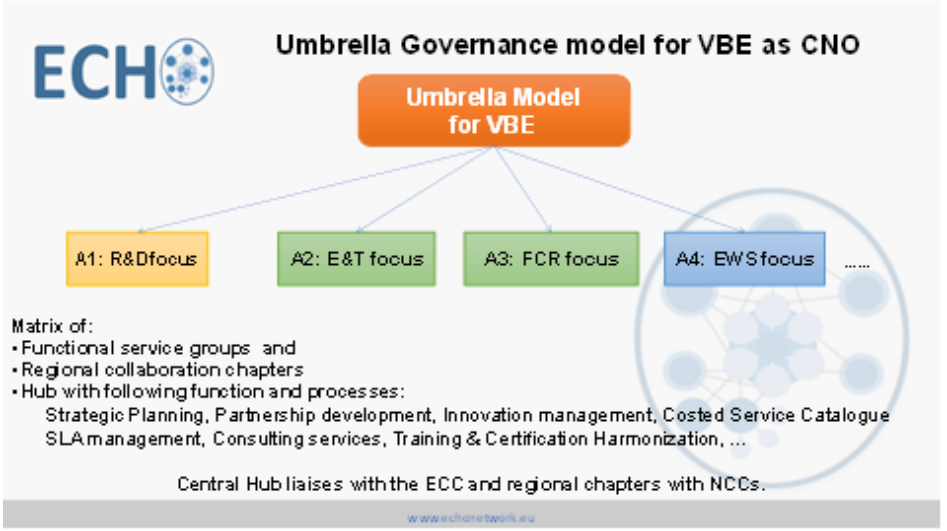

Figure 5: Defining A0 as "over and above" the A1-A4 agreed processes and structures, delegated by functional groups and regional chapters to the central hub.

The development of A0 is based on the assessment of A1-A4 and their sensitivity analysis. The process was led by ECHO's WP3 and WP2 Leaders, in consultation with WP4,5,6,9 Leaders and with the involvement of T3.4. and T3.5 leaders, aiming to provide integration of expectations of the different service groups and partnership (network) development perspective, together with a link with the current status of ECHO project governance and management (reflected in the ECHO Annual Report 2019 – ECHO D3.5.A1) and current assessment of the R630 implementation.

The description of a generic A0 as it is presented in Figure 5 provides opportunity to run breeding environment, which will be able to generate virtual organisations (service or product groups) to deliver specific services and products, benefiting from the framework established by A0 for strategic and business planning, partnership development, innovation management, service catalogue management with a framework for Service Level Agreements (SLAs) and other value added services to the Network.

Matrix model of regional chapters and services organisations

The suggested CNO will cover European Cybersecurity Competence Community (see Figure 6) by communicating with European Centre of Competence (ECC) and National Coordination Centres (NCCs) as an institutional framework, and will also interface with EC and EU MS, ENISA, EDA, EUROPOL and NATO Cyber organization (NCIO).

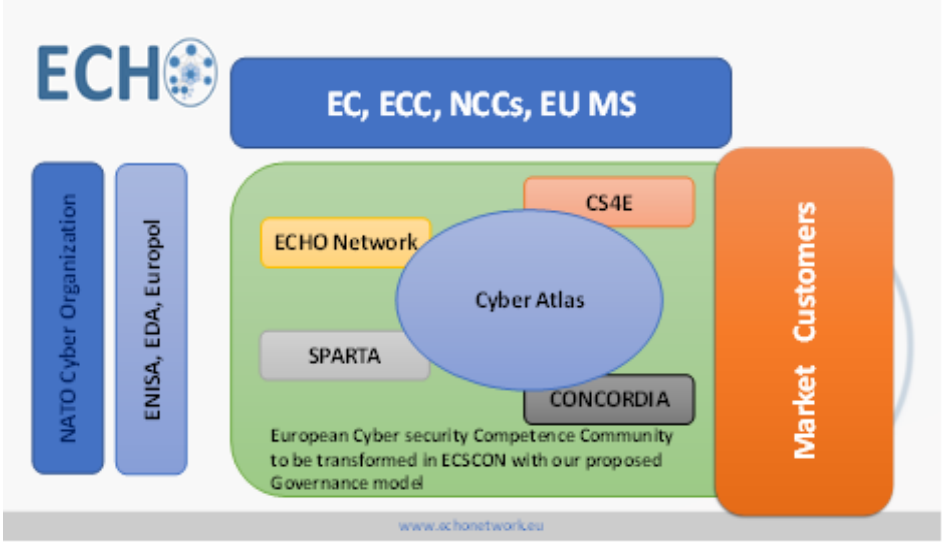

Figure 6: Framework for development of the CNO.

On the "partnership" side, the CNO will work with "market" customers, based on service (product) offering developed by the functional service groups, presented in the Catalogue of services (in the form of a "federated" catalogue).

At the core of the CNO as a breeding environment is a Matrix (see Figure 7) of regional entities (R, chapters) and functional entities (F, service groups) with a central hub, exercising the governance and agreed (delegated) central management role (C, ECSCON Hub).

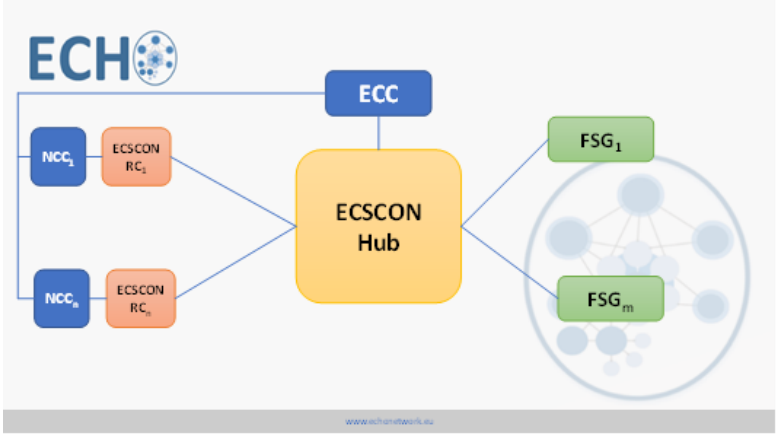

Figure 7: Matrix model for ECSCON.

Definitely, the strategic autonomy of EU is needed in the field of Cyber security, but at the same time civil-military cooperation (EU MS, EDA) and cooperation with NATO (ASG ESC, CDC, NCIO) are also required.

On institutional level Cyber security cooperation will go through ECC/NCCs and we make some assumptions and recommendations as we will also use advisory council mechanism to have our ECHO organisation aware and visible in this environment.

During the discussions, following the decision for development of A0, AFCEA and DCAF were mentioned as good examples on how does it work for a NGO and non-for-profit organisations. ECSO is a great example in Public-private Partnership environment, so the development teams will design in ECHO D3.3 suitable model, inheriting good practices from all spheres of operations.

Organisational levels

The regional-focus groups' dimensions can be seen as a high-level coordination matrix of resources to services and products of the umbrella organisation, delivered mostly by service-focused groups.

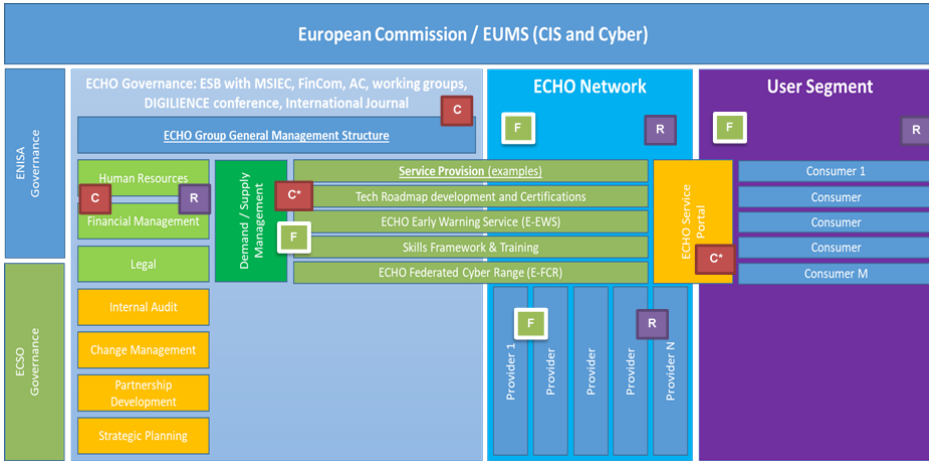

Figure 8: ECHO Target Operating Model (TOM) and organisational levels.

In terms of ECHO Target Operational Model (TOM), provided as part of the work on ECHO T3.5, the two dimensions of the matrix are illustrated in Figure 8.

The organisations with umbrella-wide governance and management functions are designated with letter "C" (Central). These functions are maintained in order to provide the stability of goal, mission, vision, as well as governance and management compliance across the network.

The compliance is based on several products of negotiation and agreement process among member organisations – documents such as strategic and annual plans, services catalogues and others. These documents are related to benefits and resources sharing and also common provision of services and products.

The "C*" means mainly monitoring and controlling functions of the central authorities over the activities provided by the Regional and Focus levels.

The regional aspects of the TOM can be seen in boxes designated with letter "R" (Regional) in Figure 8 and services (sectoral, focus group on services) aspects can be considered in boxes designated with "F".

Regional hubs have to alleviate and assure the overall administrative function of the central level (left part of Figure 8) and focus groups should provide capabilities, competences and capacities for services provision.

The matrix is established between Regional structures and Functional structures in a CNO with certain Central elements.

There is a level of independence of Regional and Functional elements of the CNO, but the synergy is provided by the Central elements which are justified by the mandate provided by Regional and Functional elements with opportunity to establish new Functional and Regional elements.

More stable from organizational perspectives are the Regional elements, that in R630 context will be associated with the NCC of the member-states. Functional elements are type of Virtual Organisations established for delivery of specific services (CHECKs in the terminology of CS4E). Some universal services could be maintained by the Central hub for standardisation and compliance in closer cooperation with the EC and ECC.

Membership and representation

The flexibility of decisions provided to regional focus groups should be considered from the point of view of the actors and structures involved in the processes. Their rights and representation should be also considered. A possible solution is to divide members according to their commitment to the network.

The umbrella type of organisation with regional and focus groups should have at minimum the following membership categories:

- *Accredited member* – certified organisation or individual for cybersecurity competences, benefiting from reputation gained, without any voting rights;
- *Associated member* – member associated to regional chamber with voting rights to the chamber's structures. Commitment of this category of members is related to provision of recourses and organisation of regional level events and activities. (The expected level of commitment should be further specified);
- *Full member* – member with full commitment both to the regional level and to network services.

Representation in legislative bodies on central level – General Assembly or General (Annual) Meeting – should be ensured for the full members and for representatives elected from the regional bodies (hubs, chambers or chapters) of the ECHO organization. Flexibility in management operations should be ensured by procedures describing the interactions of regional and service dimensions of the organisation.

Key decisions to define the umbrella organisation

Based on the results from the Workshop and the decision taken to define A0 as an umbrella governance model for ECHO organisation, the decision points shown in Table 1 were identified. These points were further discussed in order to identify preferable decisions for the A0 development.

Having these high-level descriptions of key decision points which have to be included in development of Alternative 0, analysis of the relationship between decision criteria and key decision points was conducted. On its basis, the *Common elements from four alternatives* were identified in order to be included in A0.

Key processes to be designed for A0

Setting up the umbrella organisation requires flexibility and coordination between central and regional or sectoral level with well-developed procedures for setting-up the VBEs (VBOs) "under the umbrella". The key processes that will assure these requirements were selected and their detail development and description will be provided by ECHO Deliverable 3.3 at the end of 2020.

The analysis of the Alternatives' common elements shows that this is done by taking several measures.

The main aim of all four alternatives was to develop appropriate level of common goal agreement, agreement on network level of competences and benefit and risk sharing.

These agreements support the level of trust about the qualities and capabilities of the members and provide a framework for development and operations of the VBEs. These prerequisites are maintained through the following measures:

a. Membership levels with mandatory and standardized requirements for network-level capabilities;
b. General agreement and per activity agreement with members;
c. Representation to the central and regional/functional bodies;
d. Assurance of high level of Accountability and Transparency in all levels.

Openness and inclusiveness is naturally achieved with creation of advisory units within CNOs' central bodies as discussion, coordination and standardisation forums. These advisory units support both governance and central management bodies – General Assemblies, Board of Directors (BoD), CEO, CFO, etc.

The expansion of the network, publicity and promotion is of great importance and is addressed through education, training and scientific events. In all alternatives there are one or several annual events. In addition, there is a specific policy of external transparency to potential customers and members that shows both the benefits and the burdens to work with the CNO.

Table 1: Decision points options and selection

Decision point	Options	Decision
Scope	**Basic**; **Interim**; **Full.**	*Interim, which provides Governance and Management Consulting; (E-GMC) and MSAF (E-MAF)*
Sub-entities	**None;** **On geographic basis;** **On thematic basis;** **Mixed**, with both geographic and thematic entities.	*Mixed as CHECKs or VOs* *Some may be legal entities*
Strategic autonomy	**Non-issue;** Applies only **to certain VOs;** Applies **to the umbrella;** Applies **to the VBE and all VOs.**	*Consult with the EC/EUMS for establishing CHECK and approval of the participants*
Types of membership	**Describe levels** of commitment to the organization.	*Individual, Institutional or Club member, Partner, Participant*
Key processes	**Identify the processes** that will be considered as critical for the success of the CNO and assess which part of them (according to the KPI for WP3) **will be further developed in D3.3**.	*Strategic and business planning; Partnership development; Catalogue management; Customer relations management;* *Innovation (R&D) management*
Key organizational structures	**Identify the organizational structures**, required for formal assignment to the processes in RACI	*GA, BoD, Committees to the BoD, Executive Management, …*

Despite the willingness to attract new members, all CNOs do not compromise the members' *compliance to network goals and network-wide competences*. The acceptance and evaluation of members is always approved at central level, even if the application process starts within some regional/functional entities. Most of alternatives have their membership committee or CNOs' scientific committee which provide requirements and oversight. On-line registers and documentation on membership status is also developed.

The strong focus on R&D and E&T of all CNOs is supported by establishing advisory committees which provide methodological support and strategic planning support.

The Catalogue of services is defined in only one of the alternatives (A3), but it can be argued that it exists in some forms in other alternatives' CNOs. Planning and coordination of the Catalogue is considered mainly as a management task. The governance part of strategic direction and agreement is provided through annual or biannual Business plan of the CNO.

Taking into account the considerations given above, key processes to consider as a first priority of selection for further development in the ECHO Deliverable 3.3 are identified as follows:

1. Strategic and business planning;
2. Partnership development;
3. Innovation (R&D) management;
4. Catalogue management and Customer Relations Management.

Table 2 presents a possible mapping of the levels of the network – its Central hub and regional or services' level.

This "map" can be further enhanced with the level of the programmes and projects (activities). These activities are conducted in collaborative manner by the partners on the regional or group level or on central level. The activities should be managed by additional per activity agreement and are targeted in actual delivery of CNO's goals, tasks and services.

The mapping in Table 2 is related, but not limited to COBIT[6] reference model. COBIT will be one of the main frameworks which will be used in ECHO D3.3 design. The logic behind follows the results of alternatives' assessment and A0 development requirements – the flexibility to adopt new objectives and fields of management within the "umbrella" of the CNO.

Further Steps in Development of the Governance Model for ECSCON

The following steps and activities should be implemented in order to finalise the Governance Model of ECSON:

1. Detailed processes design;
2. Organizational roles and structures definition;
3. Detailed Responsible, Accountable, Consulted, Informed (RACI) matrix with roles descriptions;
4. Charter the Bylaws of the organisation.

During the development of the ECSCON Governance Model following aspects should be considered and also prepared as documents:

1. Key change management initiatives and phases to be designed in the transition plan;

Table 2: Process and levels of the CNO.

Processes	Central Level	Regional or services hubs
Strategic and business planning	Ensure Governance and Management Framework Settings	Programme management
	Resource and benefits sharing	Management of performance
	Budget and Investment Mix	Planning of R&D and E&T, specialisation and resources
	Improvement and change management	Plan for capabilities and implementing changes
	Monitoring and auditing	Managed business controls and information
Partnership development	Network-Level Competences	Cooperative activities agreement and management
	Conflict resolution	Logs for members' activities
	Transparency	Information assurance and documents availability
	Information sharing, knowledge management and representation of the CNO	Knowledge Management, E&T and events
Innovation (R&D) management	Ensure network-level R&D goal consensus	Set-up group-level goals
	Managed R&D strategy	Manage compliance with the strategy
	Common budgeting and funds approval	Suggest, plan and report for group activities
Catalogue management and Customer Relations Management	Ensured Stakeholders engagement	Management of requirements
	Ensured benefit delivery	Compliance and performance
	Ensured resources optimisation	Managed capacity

2. Key tasks for internal audit to support A0 implementation through IOC and FOC;
3. Key partnership development tasks;
4. Key relations with ECC and NCCs, with ENISA, EDA, Europol as well as NATO Cyber organization.

All the task above should be conducted in close cooperation, understanding and agreement with the other Cyber security pilot projects and Cyber security Community inside and outside of the EU.

Conclusions

The analysis and activities related to the development of ECHO Project Governance model lead to the conclusion that an umbrella type of Governance model of a network organisation is suitable and can be established as a common

framework of European network organisation in Cyber security – the proposed organisation is named ECSCON.

The paper presents in brief the mandate, needs and objectives, analyses of existing CNOs' governance models and information sharing models in the collaborative network environment.

The four alternatives presented in ECHO D3.2 "Governance Alternatives" were developed with a top-down approach using a scientifically sound method of selecting among generated alternatives with a bottom up approach. The alternatives were developed in such a manner as to address four different service areas of ECHO (MSAF, Cyber Skills, EWS, FCR), thus a team of experts, working on the Work Packages related to the services was formed. All the four alternatives received similar ranking from experts and based on the final discussion during the Workshop on Governance Model Alternatives Assessment and Selection, a final decision was taken to develop an "umbrella" governance model. This governance model is expected to provide the baseline for operations of the ECHO CNO and its governance but will also leave room for a certain level of strategic autonomy for the specific groups of services. There is an initial agreement that the umbrella organization could maintain key processes and key universal services as well as coordinate the regional / national representation through the chapter type membership even for the combined European Cybersecurity Competence Community, developed under the four pilot projects, ECSO and Cyber Atlas (JRC) efforts.

With the decision for the development of an umbrella Governance model for ECHO, it is even more important to agree on the development of a White paper on governance (self-governance) of a collaborative network on cyber - for example European Cyber Security Collaborative Network (ECSCON), considered as an eco-system of entities developed under the implementation of the four pilot projects.

It will embrace participants from ECHO, CS4E, SPARTA, CONCORDIA and in cooperation with Cyber Atlas will work to strengthen the EU cyber community liaising with ECC (centrally) and NCCs on member-states level.

Next steps in collaboration could provide detailed design, transition plan and internal audit to assess the maturity of the implementation of the governance model through two stages of IOC (2024) and FOC (2026), after finalization of the four pilot projects in 2023 if not earlier.

Acknowledgements

This work was supported by the ECHO project, which has received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement no. 830943.

The authors gratefully acknowledge the work on Governance model definition of all ECHO teams and external experts who took part in the alternatives' assessment and selection process.

References

[1] European Commission, "Proposal for a Regulation of the European Parliament and of the Council: Establishing the European Cybersecurity Industrial Technology and Research Competence Centre and the Network of National Coordination Centres," COM(2018) 630 Final, 2018/0328 (COD), September 9, 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018PC0630&qid=1581323545128&from=EN.

[2] Cybersecurity Competence Network, "About," CyberCompetenceNetwork (blog), accessed July 12, 2020, https://cybercompetencenetwork.eu/about/.

[3] Luis M. Camarinha-Matos, Hamideh Afsarmanesh, Nathalie Galeano, and Arturo Molina, "Collaborative Networked Organizations – Concepts and Practice in Manufacturing Enterprises," *Computers & Industrial Engineering* 57, no. 1 (August 2009): 46–60.

[4] N.A. Antivachis and Vasilis Angelis, "Network Organizations: The Question of Governance," *Procedia - Social and Behavioral Sciences* 175, no. 12 (February 2015): 584–92, https://doi.org/10.1016/j.sbspro.2015.01.1241.

[5] Luis M. Camarinha-Matos, Hamideh Afsarmanesh, and Martin Ollus, eds., *Methods and Tools for Collaborative Networked Organizations* (Springer US, 2008), https://doi.org/10.1007/978-0-387-79424-2.

[6] ISACA, *Maximizing the Combined Effects of COBIT 5 and CMMI: A Guide to Using the Practices Pathway Tool* (Rolling Meadows, IL, USA: ISACA, 2017).

About the Authors

Assoc. Prof. Dr. Georgi **Penchev** works as a full-time lecturer at the Department 'National and Regional Security', University of National and World Economy, Sofia, Bulgaria. He is teaching courses on Defence and Security Economics, IT in Nuclear Security, Defence Acquisition and other security related courses. He took part in several national and international research projects, including projects funded by NATO and EU programmes.

Antoniya **Shalamanova** holds a Bachelor degree from the American University in Bulgaria with double major in Political Science and International Relations and Business Administration. She is a Master of Arts in Conflict, Security and Development from King's College London. After a number of internships in the Bulgarian public administration, in the last 9 years, Antoniya pursued a career in the private and NGO sectors working mainly in the project management sphere.