Multimedia Tools and Applications (2022) 81:9431–9443
https://doi.org/10.1007/s11042-021-11109-2

1180: CYBERSECURITY, INTELLIGENT MULTIMEDIA SYSTEMS FOR THREAT DETECTION AND DATA PROTECTION

Business, Organisational and governance modalities of collaborative cybersecurity networks

Todor Tagarev[1] · Bríd Á. Davis[2] · Michael Cooke[2]

Received: 24 October 2020 / Revised: 12 May 2021 / Accepted: 28 May 2021 /
Published online: 5 June 2021

Abstract

Countering advanced cyber threats requires investments in awareness and qualified personnel, as well as advanced technological solutions. Very few companies have the competencies and capacity to attempt to provide comprehensive solutions and sustain the technological drive and skill levels. Novel organisational solutions are needed to deliver advantages vis-à-vis both threat actors and competitors. The European Union sees one potential solution in the establishment of a network of cybersecurity competence centres. Starting in the beginning of the centuy, the creation of collaborative networked organisations in other fields demonstrated significant benefits in sharing knowledge, resources, and risk to exploit quickly emerging market opportunities. The major challenge in creating networked organisations is to provide long-term, effective collaboration through adequate governance and management. To support the elaboration of a solid governance model of a cybersecurity competence network in a Horizon 2020 research project, this article presents the results of a study of 92 existing network organisations working in cybersecurity and closely related fields. It presents the implemented methodological approach, the identification of main types of business models depending on funding streams and the degree of coordination among partners, organisational modalities, and prevailing governance models depending on member representation on senior governance bodies.

Keywords Cybersecurity · Collaborative networked organisation · CNO · Organisational modalities · Business model · Governance requirements · Governance model · ECHO project

✉ Todor Tagarev
tagarev@bas.bg

Bríd Á. Davis
Brid.Davis@mu.ie

Michael Cooke
Michael.Cooke@mu.ie

Extended author information available on the last page of the article

1 Introduction

As cybersecurity is increasing in importance in the lives and activities of all people in society, not least professionals working in complex organisational systems providing services and maintaining critical infrastructures across all key sectors in the economies of Europe, the need for new technological solutions and dedicated training and awareness education is of increasing importance [3, 9, 13]. The cybersecurity threats that face us today are too ubiquitous and transnational in nature for individual organisations, corporations, and even nation-states. Collaboration and cooperation are needed to enhance the security and resilience to common threats from cyberspace [15, 20], especially those that target multiple sectors concurrently and have the potential for cascading effects due to interdependencies between sectors [11, 19].

This issue has been addressed within the EU through the establishment of a programme orientated towards the creation of a Europe-wide cybersecurity ecosystem based on the principles of safety, security, and openness, recognising that the solution to the common threats faced by national authorities and private organisations needs a response that can rely on the sharing of data on risks, threats, and best practices [6, 14] . Recognising this need and opportunity to harness the expertise throughout the Union, the EU established through the Horizon 2020 programme call SU-ICT-03-2018 an initiative to harmonise and synergise on the current and emerging capabilities and capacities throughout Europe and embark on the integration of networks of expertise. Emerging from this call is the cluster of four pilot projects that constitute "Cybersecurity Competence Networks," one of which is the ECHO project consisting of 30 partners from 14 European states [8] . ECHO is an interdisciplinary consortium of cybersecurity practitioners, end-user stakeholders, small to medium enterprises, industry representatives, academics. The consortium's specific sectoral concerns cover energy, transport, defence, space, and health systems. Compared to the other three projects—CyberSec4Europe, SPARTA, and CONCORDIA—ECHO puts a strong focus on the governance of the competence network. This attribute of the ECHO project is of particular importance to the ambitions of the EU initiative. Hence, ECHO includes a dedicated work package aiming to assess current governance practices, elaborate current and future needs, explore options for the governance model, identify and implement an optimal model to support the development of a Europe-wide networked organisation based around ECHO.

Towards that goal, the research team conducted a comprehensive study of the needs and objectives of the governance of networked organisations, their business and governance models. The study included interviews with representatives of two main groups of stakeholders – funding organisations and potential major customers, analysis of norms and regulations, academic sources, and existing networks.

This article elaborates on the approach to the analysis of existing networked organisations. It will present and discuss the results of the ECHO governance-related research activities, and in particular 1) the study of the range of current business models, 2) the identification of organisational models for collaborative networked organisations (CNOs) with a higher degree of complexity, i.e., incorporating various thematic activities and national or regional units, with a particular interest in CNOs serving as a "Virtual Breeding Environment" [4], and 3) their current governance models.

The central objective is to analyze existing networked organisations to support the design decisions in the creation of a multi-national cybersecurity competence network involving diverse participants – public research and technology organisations, universities, high-tech companies, and foundations. Thus, the current article focuses on the results derived from the quantitative analysis of 92 existing networks (descriptive data in the first instance, which was then categorised and measured). Section 2 outlines the methodological foundation of the study. Section 3 presents statistical results on business models, allowing to identify two clusters corresponding to models most often implemented in practice. Section 4 focuses on identifying organisational models of CNOs with a higher degree of complexity, i.e., incorporating various thematic activities and national or regional units, with a particular interest in CNOs serving as a "Virtual Breeding Environment," while Section 5 presents the findings on governance models, i.e., the primary considerations or 'dimensions' for presenting the governance model of a networked organisation and identified clusters. The final section concludes the article, outlining the main directions of follow-on use of the study results.

This article is an extended version of a paper presented at the 2020 Multimedia Communications, Services & Security conference (MCSS'20) that took place in Krakow, Poland, from 8 to 9 October 2020 [17]. In particular, this article has been enriched by a more detailed elaboration of the methodological approach and presents the study on CNOs' organizational modalities over the set of existing networks in section 4 below.

2 Methodological approach

This study was organised in terms of four phases, including 1) preparation, 2) preliminary analysis, 3) secondary analysis, and 4) aggregation (Fig. 1). The first phase involved examining project documentation, the literature on governance, and the gathering of consortium expertise on the range of issues linked with network governance, business models, and CNO coordination and management. The broad range of knowledge and experience within the consortium was considered sufficiently broad to support a representative collation of the issues that would be subject to subsequent validation, elaboration, and diversification. Internal brainstorming, drafting, and validation activities were carried out iteratively to identify redundancies and additions and ensure a strong baseline of issues resulting in a consolidated draft in Excel to structure the analysis of CNOs. Further validation was conducting through piloting by six ECHO partner organisations who analysed twelve networks. This resulted in a final template containing 17 governance issues and questions and the main parameters of

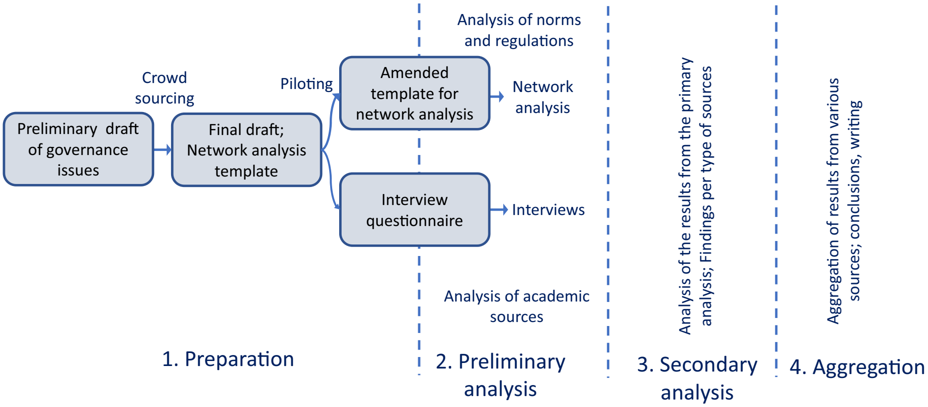
Analysis of norms and regulations
Crowd sourcing
Piloting
Amended template for network analysis
Network analysis
Preliminary draft of governance issues
Final draft; Network analysis template
Interview questionnaire
Interviews
Analysis of academic sources
Analysis of the results from the primary analysis; Findings per type of sources
Aggregation of results from various sources; conclusions, writing
1. Preparation
2. Preliminary analysis
3. Secondary analysis
4. Aggregation

Fig. 1 Methodological approach

business and governance models to be discussed with the networks in subsequent phases. Administrative information on the nature of the networks and contacts was also included.

The preliminary analysis in Phase 2 involved the analysis of a total of 92 networks within the EU, the wider European continent, and the rest of the world to allow for the broader and most robust range of models and practices to be incorporated. These were categorised into four network types:

- Collaborative networked organisations (CNOs) active in the field of cyber or information security
- Cybersecurity incubators, accelerators, tech parks, ecosystems
- Other research-intensive networks;
- Networked organisations providing information services (among others) related to cybersecurity.

A complete list of networks contained over a hundred candidates for analysis, some of which lacked sufficient publicly available data. In these cases, other networks were proposed by partners fitting the requirement of meeting the description of CNO, defined as “a network consisting of a variety of entities (e.g., organisations and people) that are largely autonomous, geographically distributed, and heterogeneous in terms of their operating environment, culture, social capital and goals, but that collaborate to better achieve common or compatible goals, thus jointly generating value” [5] . Excluded from the analysis were networks identified as being part of a larger hierarchical organisation, although they may have possessed specific expertise or capabilities in cybersecurity.

In this article, we focus on the results of the secondary analysis of the data gathered through the preliminary analysis of existing networked organisations.

3 Business models and patterns

The business models used by existing networked organisations can be presented in a two-dimensional space, with the degree of coordination of member organizations’ operational and development activities in one dimension and a combination of their profit (or non-profit) orientation and primary funding streams in the other.

3.1 Business models: Dimension 1 - degree of coordination

In this section, the different values under the heading ‘Degree of coordination’ are outlined. Service provision and product sales activities, which includes within that process the exchange of relevant information, contracting, and the management of contracts, can be imagined as a spectrum ranging from a single centralised point on the one end to more or less completely decentralised systems on the other, as summarised below:

- a single, centralised point for the provision of services and sales of products;
- a designated point of contact (POC; responsible organisation) for each main service or product;
- multiple points of contact (lead organisations) for each of the main services and/or products;

- the decentralised structure whereby each CNO member contracts the delivery of products and services for the network.

All of the qualitative data gathered in relation to the degree of coordination (i.e., in the provision of goods and services) were assessed according to their respective categorical labels. Data relating to the degree of coordination for 45 CNOs were incomplete and were excluded from subsequent analysis. A pie graph (Fig. 2) was generated to show how the distribution of product and service provision was interconnected with network development decisions for the other remaining 47 CNOs.

Most of the CNOs provide products and services via a single centralised point making up 57% of the sample ($n = 27$). This indicates that for a majority of the surveyed CNOs, the provision of goods and services was coordinated at the network level rather than through different points of contact or coordinated by various CNO members (who have standalone autonomy).

Also, but not to the same degree, 19% of the analysed CNOs used one designated point of contact for every main service/product ($n = 9$), while 17% of the sample positioned each CNO member to contract network products and services ($n = 8$).

3.2 Business models: Dimension 2 – Profit orientation and funding streams

The second dimension looked at the relationship between different CNO funding or revenue streams on the one hand and profit/non-profit orientation on the other with respect to their business models. For this purpose, an arbitrary numerical scale was developed in order to map these aspects of the business model on each of these variables, as represented in Table 1 below.

For the purposes of this article, the term "commercial" implies revenue or funding that is primarily derived from the selling of products and services. The use of the adverbs 'exclusively,' 'primarily,' and 'balanced,' while subjective, nonetheless allow for a useful comparative assessment as they are not regulatory terms, nor do they feature in statutory documentation.

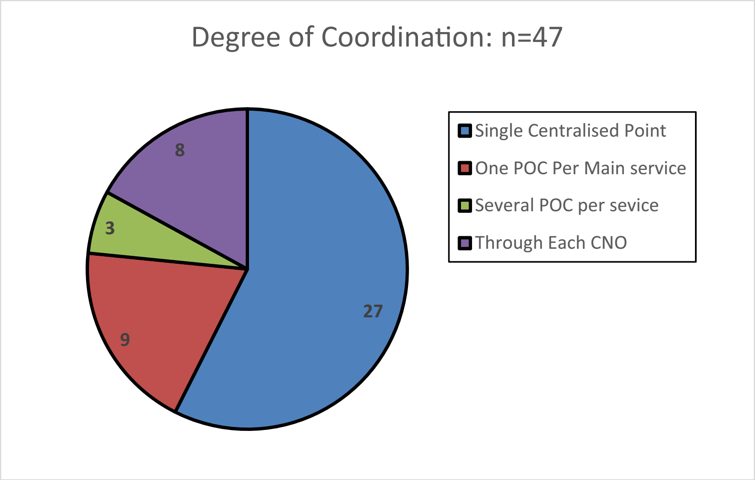

Fig. 2 Degree of coordination among CNOs

Table 1 Existing networks: Profit and funding streams, scale from −5 to 5

Profit orientation *Funding streams*	Non-for-profit	For-profit
Exclusively /entirely/ public funding	5	Not applicable
Primarily public funding	3	1 (unlikely)
Balanced funding streams	1	−1
Primarily commercial funding	- 1 (unlikely)	−3
Exclusively commercial funding	Not applicable	−5

All of the qualitative data gathered concerning the profit-orientation and funding streams were assessed in line with the categorical labels presented above.

Data relating to the profit orientation and funding streams for 32 CNOs were unavailable and so were excluded from subsequent analysis. Among the sixty CNOs that remained, a total of 53 were determined to be not-for-profit, with seven deemed as for-profit networks.

Most of the *not-for-profit* CNOs worked with “balanced funding streams,” which means a mix of commercial and public funding. These made up 41% ($n = 22$) of the sample. Public funding relates to the national government or EU grant funding; commercial funding also includes business revenue, sponsorship, and donations. Exclusive reliance on public funding comprised the second largest funding model category, accounting for 36% of the sample ($n =$ 19).

Most of the for-profit CNOs relied exclusively on commercial revenue accounting for 71% of the sample ($n = 5$). Nevertheless, there were examples, although few ($n = 2$ at 29%), of for-profit CNOs, utilising a balanced funding stream with a somewhat equal mix of public and commercial sources.

3.3 Visualisation of CNO business models

The data analysis involved using IBM SPSS™ 25 to carry out a contingency table analysis to examine the link between Dimension 1 and Dimension 2 above. It was determined that regarding the ‘degree of coordination’ classification, most of the existing networks were not-for-profit, relying solely on public funding ($n = 11$; 23%), or on a balanced funding stream ($n = 6$; 13%) operationalised under the constraints of a single process-single centralised point.

The findings show that of the 92 CNOs that were examined, the provision of services and sales of products tends to be coordinated via a single centralised point, regardless of whether this relates to the exchange of information with customers, contracting, or contract management. Furthermore, these organisations depend on either public funding exclusively (i.e., government/EU grants, etc.) or a more or less equal ratio of commercial and public funding. See Fig. 3 below for a visual display of these findings.

4 Organisational modalities of collaborative networked Organisations

The analysis of existing collaborative networks allowed the exploration of more complex organisational modalities, where the CNO involves one or more types of legal entities of a different type.

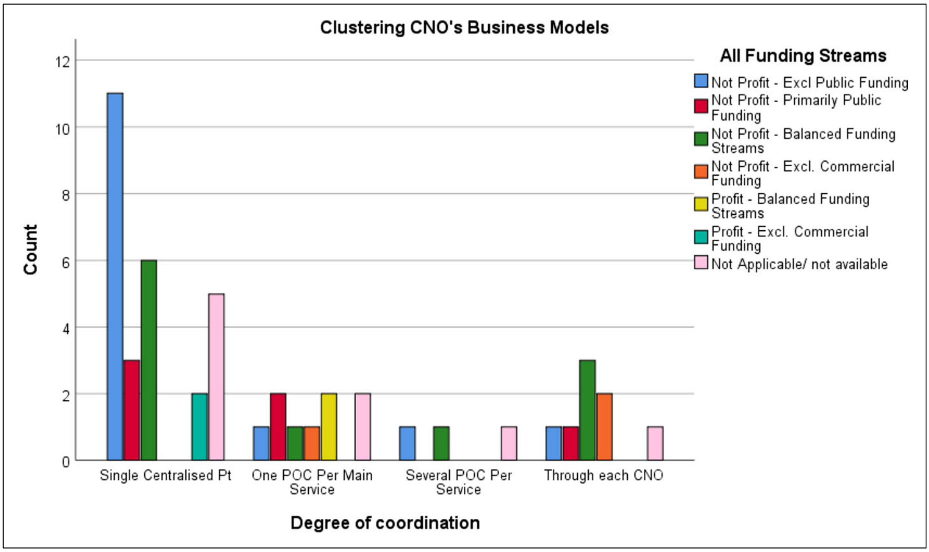

Fig. 3 Clustering CNO's business models – Profit and funding stream vs. Degree of coordination

In nearly 80% of the cases, the analysed networks are registered as non-for-profit legal entities – alliance, association, group, 'partnership,' 'institute,' etc. (Fig. 4). Other 8 % are registered as corporations, private limited liability companies, or private institutes, while nearly half of that percentage is formed by 'accelerators' providing seed funding for start-ups or investment funding for existing companies.

Another 12% are not registered as legal entities. They are formed as a 'programme' or an initiative of an existing organisation or function on the basis of an agreement, often an

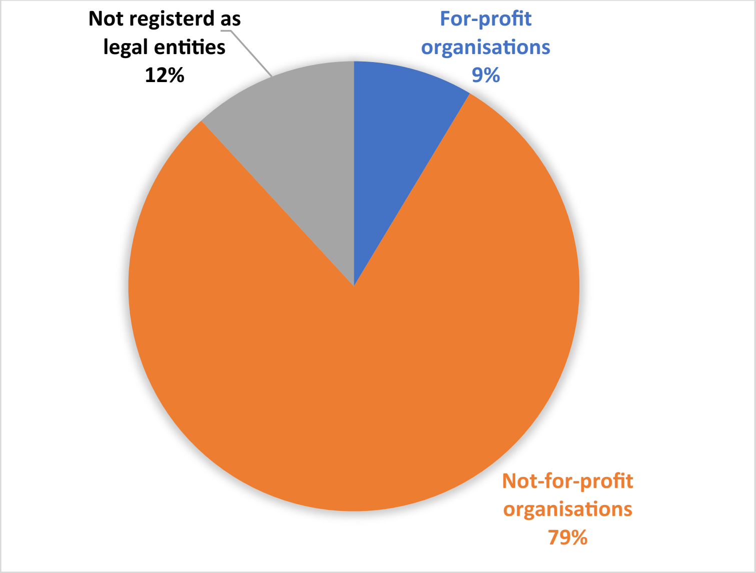

Fig. 4 Registration forms of CNOs

international agreement, designating an organisation serving as the legal entity representing the network. An example for the latter is provided by the 12 CapTechs (Capability Technology Areas) moderated by the European Defence Agency (an intergovernmental agency of the Council of the European Union [7]) and bringing together experts from government, industry, small and medium enterprises (SME), and academia to focus on particular technologies related to different military domains.

Of higher interest for the future evolution of the ECHO network, and the European network of cybersecurity competence centres more generally, are existing organisational collaborations where the CNO includes or is related to one or more types of constituent legal entities. In total, 47 of the explored networks have such units (see Fig. 5):

- 27% of the CNOs have thematic units;
- 17% have regional units; and
- 9% have associated virtual organisations,

while five of the CNOs have both thematic and regional units, and one has both regional units and an associated virtual organisation.

Twenty-five of the explored networked organisations have distinct, thematically oriented units. The overwhelming majority of these—special interest groups, committees, innovation communities, working groups, engagement areas, ‘podlings,’ working streams, etc.—are not legal entities. Only in two cases of networks of research and technology organisations—the Bulgarian Academy of Sciences and the Italian Consortium – Telecommunications (CNIT)—the institutes and laboratories specialized in areas of research are registered as legal entities, each one with its representatives on the governance bodies of the network.

The situation with the national or regional units is the opposite. Of the 16 networks with such units, in 14, the regional associations or chapters are registered as legal entities, and only in two the regional associations and groups are not distinct legal entities. In both cases, the relations between the umbrella CNO and its regional units are governed by the CNO’s bylaws.

On many occasions, successful cooperation leads to the creation of new organizations in the form of alliances or joint ventures [12]. One can assume that many of the explored

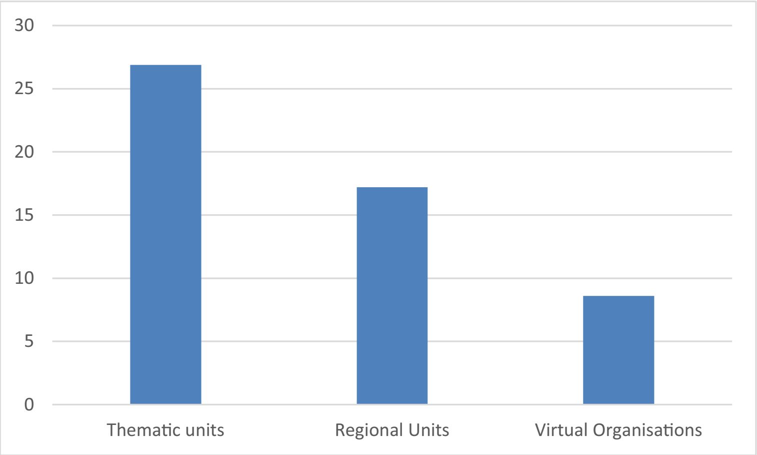

Fig. 5 Percentage of the explored CNOs that have thematic, regional units, or associated virtual organisations

collaborations have served that purpose on an ad-hoc basis. Yet, of highest interest in creating a new collaborative networked organisation in the field of cybersecurity is when the CNO serves as a Virtual organisation Breeding Environment (VBE) and CNO governance bodies decide to create a new Virtual Organisation (VO). This decision establishes rights and responsibilities for the use of intellectual property rights and other resources of the network, funding, income distribution from the activity of the VO, etc.

The VOs are of two main types [2, 18]:

- opportunity-driven VOs aiming to exploit an emerging market demand;
- virtual networked organisation for continuous delivery of a product or service, e.g., a federated cyber range or a supply chain.

Eight of the explored CNOs have associated virtual organisations of one of the two types, born out of the CNO. The study provided examples for three of the four possible combinations between a CNO, serving as a 'breeding environment,' and the virtual organisation in terms of their profit orientation (Fig. 6).

In the prevailing pattern, with five of the identified cases, the CNO is of a non-for-profit nature, while the virtual organisation, created by the CNO, is business-oriented and serves to exploit a particular product or service developed within the CNO through commercial sales.

In two cases, both the CNO and the VO do not aim to generate profit but find suitable arrangements for exploiting a particular service. An example here is the Educational Foundation of AFCEA International [1].

Of particular interest is the case with HITRUST, originating as the Health Information Trust (HITRUST) Alliance, a not-for-profit organisation. The HITRUST Alliance delivered the HITRUST Common Security Framework (CSF). Currently, HITRUST is a private company, including a for-profit division (HITRUST Services Corp.) and a not-for-profit division (HITRUST Alliance) [10].

Any of the combinations outlined in this section is of interest for designing a collaborative networked organisation in the field of cybersecurity.

5 Prevailing governance models

Key indicators related to CNO governance models were assessed involving the identification and analysis of two key dimensions. The first (Dimension 1) relates to representation on senior

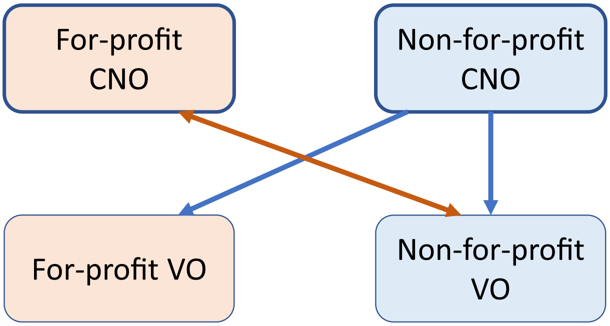

Fig. 6 Combinations between CNOs and VOs in terms of profit arrangements

governance body/ies. The second (Dimension 2) examines the decision-making principles involved in governance practice.

A two-dimensional scale was developed in order to classify both dimensions. The second step involved plotting the data to identify governance models commonly in operation.

Dimension 1. Representation on senior governance body/ies:

1. Representation involving a handful of core members;
2. Representation involving a select group of actors corresponding to certain criteria, such as founding members or members that meet specific requirements associated with scale or key roles (e.g., the project management team of a Horizon 2020 project);
3. Broad representation, or an open system whereby members may be selected through a vote by all CNO members, without specific additional criteria;
4. All participating CNO members are represented (e.g., a General Assembly of a Horizon 2020 Consortium with their nominated representatives).

Scale for Dimension 2. Decisions of CNO bodies are taken by:

1. A simple majority, requiring just over half of the weighted votes of members;
2. A qualified majority, e.g., over two-thirds of the weighted votes of CNO members;
3. A simple majority (i.e., over half of the votes cast), with each vote carrying equal weight;
4. A qualified majority (e.g., two-thirds of the votes), with each vote carrying equal weight;
5. Consensus.

Note: The weighting of votes can be based on different criteria such as CNO size as measured by numbers of personnel or annual financial turnover, or the level of financial contribution to CNO expenditure.

The analysis of the data involved using IBM SPSS™ 25 to conduct a (crosstabs) contingency table analysis to examine the link between Dimension 1 and Dimension 2. By combining and critically reviewing the findings for each type of profit orientation (i.e., for-profit and not-for-profit), it was possible to ascertain that *universal CNO representation* seems to be the most widely employed form of representation on senior governance bodies, making up 43% of the sample ($n = 26$). Similarly, the most common means of making decisions employed by all CNOs (regardless of profit orientation) was by a *simple majority (*i.e.*, over half of votes cast), with each vote carrying equal weight,* at 30% ($n = 18$).

Moreover, 15% of the sample worked on the basis that *All participating CNO members are represented*, *with an equal vote for each CNO member* ($n = 9$), followed in turn by CNOs employing a *Broad representation* approach at 10% ($n = 6$). Each used a *simple majority voting system (with over half of the votes)*. These findings are presented graphically in Fig. 7.

6 Conclusions and way ahead

By analysing existing CNO networks, with their publicly acknowledged governance objectives, practices, and requirements and the information related to their business and governance models, we can gain a good understanding of the prevailing practice. Such an analysis provides useful insights regarding the governance needs and priorities of CNO organisations

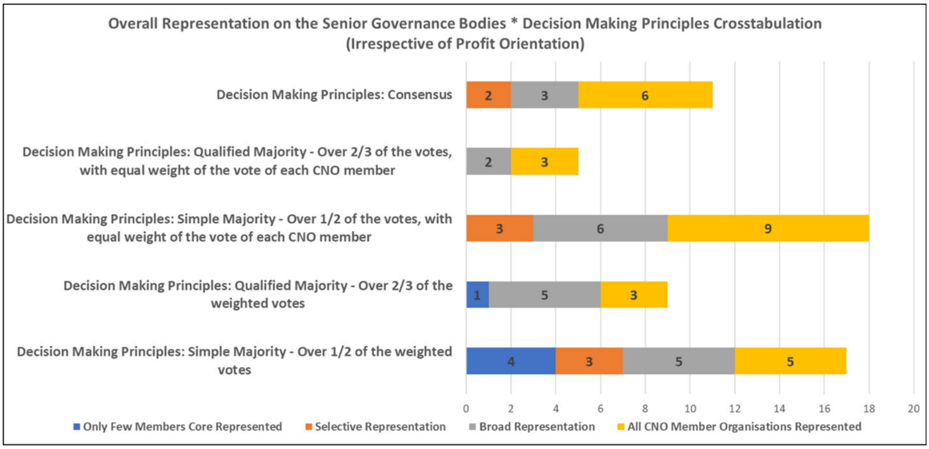

Fig. 7 Stacked bar graph demonstrating the distribution of representation on the senior governance bodies vs. decision-making principles (irrespective of profit orientation)

and allows us to observe more directly the actual – as opposed to abstract, theoretical, and prescribed – governance models of CNOs.

Also, by analysing existing cybersecurity and related networked organisations, the authors were able to establish a range of different organisational modalities of relevance for the design and maintenance of the ECHO network once established. The main emphasis has been on assessing cases where a new virtual organisation is deliberately created by the CNOs, in those cases when the CNO serves as a "Virtual Breeding Environment," and governing the relations between the CNO and the VO in such cases.

Concerning business models, the findings of the current study would seem to point to the fact that most cybersecurity CNOs operated, in terms of providing products and services, by way of a single centralised point. This finding tells us that for most of the surveyed CNOs, providing goods and services involved coordination by the network itself. Notwithstanding this finding, the fact that other, alternative modalities exist means that future networks will need to determine for themselves which structures and processes are most suitable for them and their members with respect to their own specific objectives and priorities.

In the same vein, regarding governance models, this study observed that *universal CNO representation* seems to be the most common form of representation model on senior governance bodies (regardless of profit orientation or funding stream). Moreover, the most common model adopted by CNOs regarding decision-making practices was the *simple majority model, with over half of the votes cast, whereby votes from each CNO member carried equal weight*. However, there are other models in use and therefore subject to consideration by future networks with respect to their needs and requirements. Following from these results, current and future networks need to consider how members will be represented on the CNO's senior governance bodies, as well as how decision-making is to occur, in order to achieve strong and effective collaborative structures for sustaining and growing the network.

In a follow-on study, the findings from current networks were aggregated, along with an examination of norms and regulations and a broad range of literature incorporating approximately sixty publications, combined with the analysis of interviews with key stakeholders. This mix of methods allows us to approach the topic of governance from multiple angles enabling a more rounded and thorough examination of the issue in relation to the ECHO project's objectives and the network that will emerge from it. Specifically, this means identifying best-practices in terms of elaborating and implementing governance models of CNOs; collating and clustering examples of good business and governance models of current well-functioning networks in order to propose potential alternatives in the context of the developing ECHO research; and guiding the prioritisation of governance needs and objectives [16].

In conclusion, what has been presented here in terms of findings related to best practice, governance model clustering, and relevant organisational models, is intended to guide and steer the development and evaluation of new, alternative governance models consistent with the needs and characteristics of the ECHO network, that can form the foundation for a robust, adaptable, and sustainable governance model.

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 grant agreement no. 830943. The authors gratefully acknowledge the contribution to the primary analysis of existing networks by fellow researchers from the Bulgarian Defence Institute, the Centre for Research and Technology Hellas (Thessaloniki), the European Software Institute – Centre Eastern Europe (Sofia), the Institute of ICT of the Bulgarian Academy of Sciences, Link Campus University (Rome), RHEA Group, Semmelweis University (Budapest), Telefonica Moviles Espana SA, Tallinn University of Technology, Vitrociset Belgium, and Zanasi & Partners (Modena).

References

1. AFCEA Educational Foundation, https://www.afcea.org/site/educational-foundation. Accessed 20 October 2020.
2. Afsarmanesh H, Camarinha-Matos LM (2009) On the classification and management of virtual organisation breeding environments. Int J Inf Technol Manag 8(3):234–259
3. Amanowicz M (2020) Towards building National Cybersecurity Awareness. Intl J Electron Telecommun 66(2):321–326
4. Camarinha-Matos LM, Afsarmanesh H, Galeano N, Molina A (2009) Collaborative networked organizations – concepts and practice in manufacturing enterprises. Comput Ind Eng 57(1):46–60
5. Camarinha-Matos LM, Afsarmanesh H, Galeano N, Molina A (2009) Collaborative networked organizations – concepts and practice in manufacturing enterprises. Comput Ind Eng 57(1):46–60. https://doi.org/10.1016/j.cie.2008.11.024
6. European Commission (2018) 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. A contribution from the European Commission to the Leaders' meeting in Salzburg on 19-20 September 2018, COM/2018/630 final, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52018PC0630.
7. European Defence Agency (n.d.) Who We Are, https://www.eda.europa.eu/Aboutus/who-we-are. Accessed 19 October 2020.
8. European Network of Cybersecurity Centres and Competence Hub for Innovation and Operations (ECHO), https://echonetwork.eu/. Accessed 18 October 2020.
9. Hatzivasilis G, Ioannidis S, Smyrlis M, Spanoudakis G, Frati F, Goeke L, Hildebrandt T, Tsakirakis G, Oikonomou F, Leftheriotis G, Koshutanski H (2020) Modern aspects of cyber-security training and continuous adaptation of Programmes to trainees. Appl Sci 10:5702. https://doi.org/10.3390/app10165702
10. HITRUST Wikipedia page, https://en.wikipedia.org/wiki/HITRUST. Accessed 8 October 2020.
11. Menashri H, Baram G (2015) Critical infrastructures and their interdependence in a cyber attack – the case of the U.S. Military and Strategic Affairs 7(1):79–100
12. Prange C, Mayrhofer U (2015) Alliances and joint ventures. International management 6. doi: https://doi.org/10.1002/9781118785317.weom060007.

13. Radunović V, Rüfenacht D (2016) Cybersecurity competence building trends. Research Report. DiploFoundation, https://www.diplomacy.edu/sites/default/files/Cybersecurity%20Competence%20Building%20Trends%20in%20OECD.pdf. Accessed 19 October 2020.
14. Sharkov G (2016) From cybersecurity to collaborative resiliency. Proceedings of the 2016 ACM workshop on automated decision making for active cyber defense, 3-9, doi: https://doi.org/10.1145/2994475.2994484.
15. Taddeo M (2019) Is cybersecurity a public good? Minds Mach 29:349–354
16. Tagarev T (2020) Towards the Design of a Collaborative Cybersecurity Networked Organisation: identification and prioritisation of governance needs and objectives. Future Internet 12(4):62. https://doi.org/10.3390/fi12040062
17. Tagarev T, Davis BA (2020) Towards the Design of a Cybersecurity Competence Network: findings from the analysis of existing network Organisations. In *Multimedia Communications, Services and Security*, MCSS 2020, edited by Dziech a, Mees W, Czyżewski a, Communications in Computer and Information Science, vol. 1284. Cham: Springer, 37–50, doi: https://doi.org/10.1007/978-3-030-59000-0_4.
18. Tagarev T., Yanakiev Y (2020) Business Models of Collaborative Networked Organisations: Implications for Cybersecurity Collaboration. In: *Proceedings* 2020 *11th IEEE International Conference on Dependable Systems, Services and Technologies, DESSERT 2020*, Kyiv, Ukraine, May 14-18, 2020, pp. 431–438, doi: https://doi.org/10.1109/dessert50317.2020.9125011.
19. Talton E, Tonar R (2018) A lack of cybersecurity funding and expertise threatens US infrastructure. Forbes Magazine, 23 April 2018, https://www.forbes.com/sites/ellistalton/2018/04/23/the-u-s-governments-lack-of-cybersecurity-expertise-threatens-our-infrastructure/. Accessed 18 October 2020.
20. Weiss M, Jankauskas V (2019) Securing cyberspace: how states design governance arrangements. Governance 32(2):259–275

Affiliations

Todor Tagarev[1] • Bríd Á. Davis[2] • Michael Cooke[2]

[1] Institute of Information and Communication Technologies, Bulgarian Academy of Sciences, “Acad. G. Bonchev” Str., Bl. 2, 1113 Sofia, Bulgaria

[2] National University of Ireland Maynooth, Maynooth, County Kildare, Ireland