Information & Security

Y. Yanakiev
vol. 46, no. 1 (2020): 79-98
https://doi.org/10.11610/isij.4606

Published since 1998

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

Research Article

A Governance Model of a Collaborative Networked Organization for Cybersecurity Research

Yantsislav Yanakiev (✉)

Bulgarian Defence Institute "Prof. Tsvetan Lazarov," Sofia, Bulgaria
https://www.di.mod.bg/en/defence-institute

ABSTRACT:

This article presents the results of the analysis of governance and management practices of Collaborative Network Organisations (CNOs) in the Science and Technology domain. The aim is to support the process of designing a governance model of a cybersecurity network by identifying best governance and management practices of existing collaborative networks. The results presented in the article are based on the analysis of governance models of three relevant organisations: (1) NATO Science and Technology Organization; (2) the Gigabit European Academic Network; and (3) the European Defence Agency's Capability Technology Groups. The common ground is that they are regarded as CNOs with a high degree of centralisation of funding streams and a high degree of centralisation of the main business and governance decisions. The method of analysis includes a literature review and desktop research. The information sources used for the analysis are official legal documents about the CNO's governance and management, especially for potential members and customers' engagement; organisation and expected competence level and behaviour of CNOs' members; the charters, decisions, reports issued and approved by the central or regional governance bodies of the organisations.

ARTICLE INFO:

RECEIVED: 12 June 2020
REVISED: 28 AUG 2020
ONLINE: 02 SEP 2020

KEYWORDS:

Cybersecurity, Collaborative Networked Organisations, Governance Model, Science and Technology

✉ Tel.: +359 2 92 21862; Fax: + +359 2 92 21808; E-mail: y.yanakiev@di.mod.bg

Introduction

The European Union Cybersecurity Strategy: An Open, Safe and Secure Cyberspace [1] defines the cyber threat among the most important for the Union and the EU Member States (MS). To respond to this challenge the European Union aims at creating a reliable, safe, and open cyber ecosystem. Therefore, in 2018, the European Parliament and of the Council issued a "Proposal for a Regulation on establishing European cybersecurity industrial, technology, and research competence centre and a network of national coordination centres" (COM(2018) 630) The EU R630 recommends the new cyber ecosystem to include both a central governance body (i.e., a hub) and regional (or sectoral) centres.[2]

To boost the collaborative Science and Technology efforts at the European level, the European Union's Horizon 2020 programme funded four pilot projects in 2019 focused on the process of establishing European cybersecurity industrial, technology, and research competence centre and a network. The "European network of cybersecurity centres and competence hub for innovation and operations" (ECHO) [3] is one of these pilot projects. Among the main objectives of ECHO is to design and to implement a governance model of cybersecurity Collaborative Networked Organisation.

This paper presents the results of the analysis and identified best governance and management practices of Collaborative Networked Organisations (CNOs) in Science and Technology (S&T) domain. The purpose is to develop and to formulate one possible alternative for ECHO governance model based on the examination of existing relatively similar S&T networks.

The review of academic literature about business and governance models of CNOs[4] allows identifying some important characteristics of such kind of organisations that make them feasible to design a governance model of a cybersecurity network. Among the most important are: (1) flexibility, decentralized planning and control, and lateral ties with a high degree of integration of multiple types of socially important relations across formal boundaries; (2) members of CNOs are autonomous organizations that come together to reach goals that none of them can reach separately; (3) CNOs are particularly suitable for circumstances in which there is a need for efficient, reliable information; (4) in CNOs the most useful information does not flow down the command chain; rather, it is obtained from someone with whom one has had prior dealings and has found to be reliable.[5; 6; 7]

Method

To achieve the objective of the ECHO project, namely design and implementation of a business and a governance model of the network, several sequential steps have been implemented.

First, the international team from the consortium analysed the governance models of 92 selected existing CNOs based on a commonly agreed template. The team documented some key governance characteristics of these organisations like the number of members, the number of countries represented, types of partners (business, military, academia, non-governmental, etc.), legal status,

goals according to the statute, horizon of collaboration, rights and obligations of the members, decision-making process, governance and executive bodies, mechanisms for assuring fair representation on the governance bodies, external stakeholders & engagement, network engagement model, fundamental governance documents, auditing (internal and external), dispute/conflict management, ethics, transparency, etc.

Second, as a result of this initial step of the study, the ECHO team classified the analysed CNOs and identified four clusters of networks within two main dimensions: the type of funding sources (public vs. customer) and the degree of centralisation (fully centralised vs. fully decentralised).[8]

The four clusters were named as follows: (1) "A high degree of centralisation of funding streams and a high degree of centralisation of the main business and governance decisions"; (2) "A high degree of centralisation of funding streams and medium degree of centralisation of the main business and governance decisions"; (3) "Distributed and balanced funding streams (i.e., public funding and commercial sales) and a high degree of centralisation of the main business and governance decisions"; and (4) "Distributed and balanced funding streams and medium degree of centralisation of the main business and governance decisions." Additionally, these networks were analysed from the perspectives of members' representation in the governance and management bodies, as well as from their voting rules. Third, to structure the information about the governance and management practices of the analysed CNOs, the following criteria have been defined and used: (1) Scope, diversity and management of complexity; (2) Number of participants and attractiveness; (3) Stakeholders, customers and potential member engagement; (4) Maintaining the network goal consensus; (5) Maintaining the trust within the network; (6) Centralisation and horizontal links; (7) Network competences and certification procedure; (8) Risk management and shared funds. It is important to mention that the definition of those criteria is a result of joint research in the framework of the consortium, and they have been agreed among the ECHO Partners. The same criteria were applied from four ECHO teams to develop four alternative governance models based on the analysis of typical CNOs pertaining to the four distinct clusters. Fourth, following the above-defined criteria, the author analysed the key characteristics of the governance models of three typical CNOs in S&T domain that belong to the first cluster titled "A high degree of centralisation of funding streams and a high degree of centralisation of the main business and governance decisions." These are (1) NATO Science and Technology Organization; (2) the Gigabit European Academic Network; and (3) The European Defence Agency, Capability Technology Groups. Finally, the key characteristics of the analysed CNOs have been summarized from the viewpoint of their relevance for the development of a governance model of a Collaborative Networked Organization for Cybersecurity Research. The information sources used in the analysis are official legal documents about the CNOs' governance and management, especially for activities about potential members and customers' engagement; or-

ganisation and expected competence level and behaviour of CNOs' member organisations; the charters, decisions, reports issued and approved by the central or regional governance bodies of the CNOs, etc.

Results: Analysis of Governance Models of Existing Networks

The analysis of the governance models of the three existing relatively similar networks in S&T domain has the purpose to identify what is common and what is different in the governance and management practices, the perspective of collaboration, funding principles, decision-making processes, organisation and implementation of S&T activities, CNO's structure, etc. In the following rows, the main characteristics of the analysed CNOs are presented.

NATO Science and Technology Organization

The NATO Science and Technology Organization (STO) is the largest in the world collaborative research forum in the field of defence and security. In 2020, the goal of STO is to pursue long-term efforts in strengthening the Collaborative Program of Work (CPoW). This joint programme is highly attractive to experts as the network is steadily growing, today comprising approximately 6,500 scientists, engineers, and analysts originating from 30 NATO and 48 partners. They expect to have more than 300 active research teams during the year.[9]

The mission of the NATO STO is to help position the Nations' and NATO's S&T investments as a strategic enabler of the knowledge and technology advantage for the defence and security posture of NATO Nations and partner Nations, by a) Conducting and promoting S&T activities that augment and leverage the capabilities and programmes of the Alliance, of the NATO Nations and the partner Nations, in support of NATO's objectives; b) Contributing to NATO's ability to enable and influence security and defence-related capability development and threat mitigation in NATO Nations and partner Nations, following NATO policies; c) Supporting decision-making in the NATO Nations and the Alliance.

The STO aims to meet to the best advantage the collective needs of NATO, NATO Nations and partner Nations in the fields of Science and Technology.[10]

The total spectrum of collaborative S&T activities performed within the STO are promoted and managed by seven Technical Panels, each one focused on a specific technological domain. Together the seven Panels cover the complete range of defence-applied technologies. The STO Panels are "Applied Vehicle Technology"; "Human Factors and Medicine"; "Information Systems Technology"; "System Analysis and Studies"; "Systems Concepts and Integration"; "Sensors & Electronics Technology" and "NATO Modelling and Simulation Group."[11]

Main customers of NATO STO are governments, industry, academia, intelligence analysts, military and civilian researchers, security practitioners, etc.

The NATO STO closely cooperates with and supports the capability efforts of all NATO political and military structures and agencies, such as the Allied Command Transformation, the Conference of National Armaments Directors (CNAD), the NATO Industrial Advisory Group, the NATO Communications and

Information Agency, the Committee of the Chiefs of Military Medical Services in NATO, NATO Centres of Excellence, etc.

The STO's scientific and technological work is carried out by the so-called Technical Teams (Exploratory Teams, Research Task Groups, ad-hock study groups, etc.) They are temporary groups created under the Panels to perform specific activities, ranging from studies of scientific, technological or operational nature to demonstrations and technological experiments. Technical Teams activities include also the organisation of events such as research symposia, conferences and workshops.

The STO is governed by the NATO Science and Technology Board (STB), chaired by the NATO Chief Scientist, who is a high level recognized S&T leader of a NATO nation. The STB constitutes the highest authority within the STO. It is the policy body tasked by the North Atlantic Council (NAC), through the CNAD and the Military Committee, to carry out the mission of the STO, as well as exercise unified governance of NATO S&T by a) Developing and updating a long-term NATO S&T Strategy and medium-term NATO S&T Priorities; b) Obtaining endorsement for and fostering the implementation of the long-term NATO S&T Strategy and the medium-term NATO S&T Priorities, by engaging representatives of the Nations in other NATO senior committees; c) Obtaining NAC approval of the endorsed NATO S&T Strategy; d) Acting as the focal point for coordinating the STO CPoW and the S&T activities of other NATO CPoW by ensuring NATO S&T Strategy and NATO S&T Priorities alignment, by mutual awareness of activities, by avoidance of duplication and by achieving synergies.

The STO is composed of the STB, the Chief Scientist and the following three executive bodies: (1) the Office of the Chief Scientist (OCS) (NATO HQ, Brussels); (2) the Collaboration Support Office (CSO) (Paris, France); and (3) the Centre for Maritime Research and Experimentation (CMRE) (La Spezia, Italy).

The three executive bodies of the STO report to the STB which exercises the governance over these bodies.

Like all other NATO entities, the decisions in STO at all governance levels are taken by consensus.

The STO is governed by the provisions of the NATO Financial Regulations. The financial management of the STO is separate and distinct from those of other NATO bodies. The budget is submitted to the STB for endorsement and submitted to the Budget Committee for approval yearly. The STO operates strictly within the limits of the resource allocations provided and for the purposes, stipulated in the approved budget.

It is important to highlight that the principle of common funding in STO applies for the OCS and the CSO, whereas the CMRE is a customer-funded organisation. Besides, as a rule, the funding for participation of scientists in the Technical Teams is a national responsibility. There is a limited budget under the Support Programme that can be used by some NATO Nations and partner Nations for participation in the Technical Teams.[12]

Gigabit European Academic Network

The Gigabit European Academic Network (GÉANT) is a pan-European data network for the research and education community. It interconnects National Research and Education Networks (NRENs) across Europe, enabling collaboration on projects ranging from biological science to earth observation, to arts and culture. Together with European NRENs, GEANT connects 50 million users in over 10,000 institutions. Europe's NRENs are specialised Internet service providers dedicated to supporting the needs of the research and education communities within their own country.

The collaboration in GÉANT community is based on consensus-building principle.

The strategic objectives of the GÉANT association have to resonate strongly with the NRENs' strategic objectives. The strategic objectives also consider other stakeholders, including the Research and Education (R&E) community and the European Union.

The GÉANT community is committed to long-term collaboration.

The overall objective for the GÉANT partnership is to contribute to the effective European Research Area by making Europe the best-connected region in the world. To achieve this, GÉANT offers European researchers the network, communications facilities and application access that ensure the digital continuum necessary to allow them to conduct world-class research in collaboration with their peers around the world.[13]

Collaboration with GÉANT's global partners covers areas such as network performance monitoring, connectivity roaming and federated access, and real-time communications. Through the EC-funded project, the GÉANT community also collaborates with partners in Latin America, the Caribbean, North Africa and the Middle East, West and Central Africa, Eastern and Southern Africa, Central Asia and Asia-Pacific towards establishing a marketplace of services and real-time applications for international and inter-continental research groups. The GÉANT network in 2019 connected to 68 NRENs beyond its European footprint.[14]

Special Interest Groups and Task Forces help GÉANT, NRENs and other R&E bodies to collaborate, share experience and guide future developments of networking services, technology and also a variety of non-technical topics.

The General Assembly is the highest GÉANT's governing body, in which representatives of member organisations meet at least twice per year. The General Assembly elects members of the Board of Directors, which manages and administers the organisation.

There are specific committees tasked with developing policy and guidance for the Partners' Assembly on key aspects of the project such as a) The Cost-Sharing Working Group that looks at the cost elements of GÉANT services and proposes to the Assembly how these costs could be shared; b) The role of the Strategy and Innovation Committee is to develop a long-term vision, strategy and innovation agenda for GÉANT.

Weighted voting is applied at all levels of governance.

The GÉANT Association Statutes members are required to pay an annual membership fee to be determined by the General Assembly. Members may be divided into categories each of which will pay a different membership fee.

The funding comes primarily from: (1) the European Commission; (2) Membership subscriptions (NRENs and Associate members); (3) Earnings from the provision of administrative, consultancy and training services; (4) Sponsorship for specific activities.[15]

The European Defence Agency

The European Defence Agency (EDA) is an intergovernmental agency of the Council of the European Union. Currently, 26 countries – all EU Member States except Denmark – participate in EDA.

The Agency falls under the authority of the Council of the EU, to which it reports and from which it receives guidelines. The EDA is the only EU Agency whose Steering Board meets at the ministerial level. At the meetings of this governing body, Defence Ministers decide on the annual budget, the three-year work programme and the annual work plan, as well as on projects, programmes and new initiatives. The Head of the Agency is the High Representative of the Union for Foreign Affairs and Security Policy.

The Steering Board is the decision-making body of the Agency. It acts within the framework of the guidelines and guidance of the Council. The Steering Board is composed of one representative of each participating Member State and a representative of the European Commission. In addition to ministerial meetings at least twice a year, the Steering Board also meets at the level of National Armaments Directors, Research and Technology Directors and Capability Directors.

The EDA Chief Executive is appointed by a decision of the Steering Board.

Following Council Decision (CFSP) 2015/1835 of 12 October 2015, defining the statute, seat and operational rules of the EDA, the Steering Board shall take decisions by qualified majority. Only the representatives of the participating MS can take part in the vote. The votes of the participating Member States shall be weighted per Article 16(4) and (5) of Treaty of European Union.

Networks of national Points of Contacts (POCs) have an important role in the coordination of the Agency's work with the Member States: a) Central POCs (for the preparation of the ministerial Steering Board as well as organisational, institutional and budgetary matters); b) Capability POCs; c) Research & Technology POCs; d) and National Armaments Directors' POCs.[16]

The Agency has a permanent staff of approximately 170 people, but through various networks of national experts, the Agency currently involves around 4,000 defence scientists and practitioners. These networks of experts are crucial for EDA's work as they ensure coherence with national priorities.[17]

National experts are organised in Integrated Development Teams, Project Teams, as well as different Capability Technology Areas (CapTechs) which are

networking fora for experts from government, industry, small and medium enterprises (SME) and academia, moderated by EDA. Additionally, Ad-hoc Working Groups comprised of national experts can be formed for any given subject.

Currently, the Agency holds twelve CapTechs and two related Working Groups. Each of them focuses on particular technological areas associated with different military domains. The CapTechs are "Technologies, Components and Modules"; "Radio Frequency Sensors Technologies"; "Electro-Optical Sensors Technologies"; "Communication Information Systems and Networks"; "Materials and Structures"; "Ammunition Technologies"; "Aerial Systems"; "Ground Systems"; "Guidance, Navigation and Control"; "Naval Systems"; "Experimentation, System of Systems, Space, Battle lab and Modelling & Simulation"; "Chemical, Biological, Radiological and Nuclear and Human Factors." The working groups are "Cyber Research & Technology" and "Energy and Environment."

The EDA CapTechs aim to propose R&T activities in response to agreed defence capability needs and to generate projects accordingly.[18]

The Member States contribute to the Agency's annual budget according to a GNP-based formula and approve its work plan. The MS can decide whether or not to participate in Agency projects according to national needs. Likewise, the results achieved by the Agency are for the benefit of its Member States.[19]

The European Defence Agency's budget includes the general budget, the budgets associated with the ad-hoc activities and any budgets resulting from additional revenue for specific purposes. Within the framework of its mission, the Agency may receive additional revenue for a specific purpose: a) from the general budget of the Union on a case-by-case basis, in full respect of the rules, procedures and decision- making processes applicable to it; b) from the Member States, third countries or other third parties, unless the Steering Board decides otherwise within one month of receiving such information from the Agency.

The Agency implements an internal audit which is performed in compliance with the relevant international standards. The internal auditors' task is to advise the Steering Board of the Agency on dealing with risks, by issuing independent opinions on the quality management and control and issuing recommendations for improving the implementation of operations and promoting sound financial management. According to the Council Decision (CFSP) 2015/1835, the Steering Board also can appoint a College of Auditors to perform the external audit function of the administrative and operational budgets, financial accounts and financial statements of the Agency.

Comparison of the Main Characteristics of the Governance Models of the Analysed CNOs in the S&T Domain

Table 1 summarises some of the key characteristics of the governance models of the three analysed networks that can be instrumental when a governance model of a collaborative networked organisation for cybersecurity research is being developed.

Table 1: Summary of the key characteristics of the governance models of the analysed organisations

Criteria of analysis/ CNOs	NATO Science and Technology Organization (STO)	Gigabit European Academic Network (GÉANT)	European Defence Agency (EDA)
Scope, diversity and management of complexity	- *Big player* - the largest in the world collaborative research forum in the field of defence and security; - *Public S&T organisation;* - *Geographically spread* (All NATO Nations, PfP, MD and Global Partners); - *Governance bodies and Structure*: The STB and the Chief Scientist; Executive bodies: the OCS; the CSO; the CMRE. - Seven *Technical Panels*, each one focused on a specific technological domain; - *Technical Teams*.	- *Big player* - a pan-European data network for R&E; - *Geographically spread*, interconnects National Research and Education Networks all over the world; - *Public S&T* organisation; - *Governance bodies and Structure*: CNB and NRENs; - The General Assembly elects members to the Board of Directors; - *Operations Centre* mages Day-to-day S&T. - *Special Interest Groups* and *Task Forces.*	- *Big player,* an intergovernmental agency of the Council of the EU. Currently, 26 EU MS except for Denmark participate in EDA; - *Public S&T organisation;* - *Governance bodies and Structure*: EDA is a CNB, there are no regional centres; The Head of the Agency is the High Representative of the EU for Foreign Affairs and Security Policy; - The Steering Board; the EDA Chief Executive; 12 *CapTechs and* 2 *Working Groups.*
Number of participants and attractiveness	- More than 6,500 scientists, engineers, and analysts originating from 30 NATO and 48 partner nations; - More than 300 active research teams during the year 2019.	- More than 50 million users in over 10,000 institutions; - In 2019 GÉANT community connected to 68 NRENs beyond its European footprint.	- The permanent staff of 170 people. Besides, through various networks of national experts, the Agency currently involves around 4,000 defence specialists.

Stakeholders, customers and potential member engagement	- *Main customers of NATO STO* are governments, industry, academia, intelligence analysts, military and civilian researchers and practitioners.	- GÉANT collaborates with o*ther e-Infrastructures; Industry*; c) *Industry; Vertical user groups* to support their disciplines.	- *Main customers of EDA* are EU MS governments, defence industry, academia, intelligence analysts, academia and practitioners.
Maintaining the network goal consensus	- *The STO's goal:* Conducting and promoting S&T activities that augment and leverage the capabilities and programmes of the Alliance; - *The STO is a CNB* governed by the NATO STB, chaired by the NATO Chief Scientist; - *Basic governance documents*: the NATO S&T Strategy and NATO S&T Priorities; The Chapter of the STO; The CPoW; The NATO STO Operating Procedures. Decisions are made by *consensus*. *There is no weighing of votes.*	- *The overall objective* for the GÉANT partnership is to contribute to the effective European Research Area by making Europe the best connected region in the world; - GÉANT governance structure is a *combination between CNB and RNB*. - The collaboration in GÉANT community is based on *consensus-building;* - *Basic governance documents:* GÉANT's Bylaws; - *Qualified majority voting; Weighted voting is applied.*	- EDA's goal is to support MS in their efforts to improve defence capabilities. - The EDA organises its S&T priorities in different CAPTECs; - EDA is a *CNB without regional centres*; - *Basic governance documents:* Council Decision (CFSP) 2015/1835 of 12 October 2015; - The Steering Board of EDA shall take decisions by a *qualified majority*; - The votes of the participating MS shall be *weighted*.
Maintaining the trust within the network	- *Long-term cooperation*; - The *STB* decides on the Mission, Vision and Strategy.	- *Long-term collaboration;* - *General Assembly* decides on the Mission, Vision and Strategy.	- *Long-term cooperation*; - The Mission, Vision and Strategy are defined by *the Council of the EU.*
Centralisation and horizontal links (	- A *CNB with regional centres* (OCS, CSO, CMRE);	- A *CNB with regional centres* (NRENs);	- A CNB, no RNBs; - Collaboration has to be approved by the

	- Collaboration to be approved by the STO STB.	- Collaboration to be approved by the GÉANT's GA.	EDA's Steering Board.
Network competences and certification procedure	- *There are no specific procedures at the STO level to evaluate member's competencies*. The researchers representing the NATO Nations are appointed by the corresponding National authorities to participate in different Technical Teams. The level of competency is the responsibility of the Nations.	- *There is no information available for the process of Network member's competences assessment and certification procedure;* - General control over the GÉANT members' competencies development is exercised by the GA and the BD.	- There is no information available about the process of Network member's competences assessment and certification procedure; - *The MS have the responsibility to guarantee a high level of competency of the national representatives*.
Risk management and shared funds	- The STO is governed by the provisions of the *NATO Financial Regulations*; - The *International Board of Auditors* for NATO shall audit the financial statements of the STO; - *The principle of common funding in STO applies for the OCS and the CSO*, whereas the *CMRE is a customer-funded organisation.* The *funding for participation in the Technical Teams is a national responsibility.*	- *The funding for GÉANT project comes primarily from* the European Commission; Membership subscriptions; Earnings from the provision of administrative, consultancy and training services; Sponsorship. - The GÉANT Association operates within the financial budget set by the General Assembly each year; Annual membership fee.	- *The financial provisions applicable to the Agency's general budget are set out in Council Decision 2007/643/CFSP.* - The Agency shall have an *internal and external audit;* - *A College of Auditors* performs the external audit of the Agency;

The analysis of the governance models of the three CNOs in S&T domain identified a high degree of similarity among them concerning the type of funding sources, the degree of centralisation of the decision-making process, the prin-

ciples of representativeness in the governing bodies, and organisational processes and procedures, while there are some differences in the voting rules and organisational structure (CNB and RNBs). For example, all three CNOs are big players in the S&T domain, they have a long-term perspective of collaboration, and they are geographically spread with world-wide coverage. Besides, the centralisation of the decision-making process with CNB (hub) is typical for the analysed organisations. The NATO STO has established, in addition to the CNB, RNBs, while in EDA and GÉANT there is no regional structures, only national POCs. Moreover, the analysed CNOs have clear and strict financial regulations in place, as well as internal and external audit. Also, main customers of NATO STO and EDA are governments, defence industry, academia, intelligence analysts, military and civilian researchers and practitioners, while GÉANT is more focused on academia and civilian companies. Furthermore, the prevailing voting principle is qualified majority with weighing of votes for GÉANT and EDA, while in NATO STO decisions are made by consensus. Last but not least, the organisation and implementation of the S&T activities in the three organisations are similar (technical teams, working groups, task forces, etc.).

The Proposed governance model of CNO for cybersecurity research

The proposed governance model of CNO for cybersecurity research attempts to incorporate best practices of the analysed organisations as a potential candidate for ECHO governance model in S&T domain.

The governance model presented in this paper is an abstraction. It does not exist as such in real life. It is based on the identified best governance and management practices of the existing CNOs in S&T domain, focusing on their prevailing characteristics.

The suggested CNO for cybersecurity research has a legal status of Public International Science and Technology Organisation.

Scope, diversity and management of complexity

The CNO is a significant player in its sector and level of operation, namely S&T in cybersecurity. It aims at bringing together representatives of the EU MS, NATO Nations and the partners of the two Alliances.

This is a pan-European network of cybersecurity scientists and practitioners. It interconnects National Research Networks (NRNs) and Centres of Excellence (CoE) across Europe. In addition to the European partners, the CNO is opened for cooperation with other similar networks all over the world based on common interests and opportunities to share resources.

The CNO's mission is to enable collaboration in cybersecurity activities in the S&T domain to support the EU MS, NATO' and partner Nations in their efforts to improve cybersecurity capabilities.

The governance model of the CNO is centralised, non-for-profit and the organisation is funded mainly by public sources.

It follows the Virtual organisations' Breeding Environment philosophy, 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.[20]
The proposed governance model of the CNO should be able to support the activities described below.

First, the CNO organises and implements its S&T activities in different Scientific Committees, including Exploratory Teams (ETs), Ad-hoc Research Groups (AHRGs) and Research Task Groups (RTGs), which are networking settings for experts from government, industry, SMEs and academia, moderated by the CNO' central network-wide authorities.

Second, the CNO brings together cybersecurity researchers and practitioners to discuss current and future challenges to Research Symposia and Research Workshops.

Third, the CNO serves as a Point of contact and facilitator of cooperation among cybersecurity experts of the EU MS, NATO' and partner Nations. To support these activities, the CNO hosts and maintains collaborative technology tools, as well as platforms to facilitate knowledge exchange such as Cybersecurity Research Connections.

Fourth, in the area of cybersecurity training, the CNO delivers learning methodologies, training content, assessment methodologies and organizes events like Research Training Courses and Research Specialist Meetings.

Finally, the CNO prepares and publishes quarterly expert reports on current and future challenges in cybersecurity.

Number of participants and attractiveness

The CNO is a large establishment. More than 35 organisations from 30 countries are participating in the CNO. There is also an individual form of membership. More than 300 scientists, representatives of SMEs, cybersecurity experts and stakeholders worldwide participate as individual members.

Two different business models are applied in the CNO's S& activities. The first is the Collaborative business model, where the CNO provides a forum for the representatives of the EU MS, NATO nations and partners to cooperate in defining, conducting and promoting cooperative research and information exchange. The second is the In-house delivery business model where S&T activities are conducted in CNO dedicated executive body, having its personnel, capabilities and infrastructure.

Even though the CNO is a relatively new organisation, the number of participants is expected to grow rapidly to 40 countries and more than 400 participants until 2025. In the years to follow, the vision is to continue the growth of the individual members by reaching approximately 500 scientists, engineers, and analysts originating from Europe. There are also ideas to attract experts worldwide and to expand CNO's network influence boarders. It is foreseen that

shortly the CNO will start Open Call project procedures, permitting for organisations from all over the world to participate in particular types of research and education projects.

The CNO has been rethinking its Improvement Programme to organise better and to meet appropriately the future challenges and the ever-increasing demands for cybersecurity S&T services without a significant increase in expenditures and the organisational efforts.

Stakeholders, customers and potential member engagement

The CNO maintains 'Over the Horizon' as its constant and guiding principle, which is being implemented and organised under the following headings: a) Positioning; b) Innovation; c) Collaboration; d) Users; e) Services; f) People in support of Decision-Making; g) Cybersecurity and Information assurance.

The main Actors and Stakeholders that the CNO identifies as prospective collaborators are as follows: a) Governments; b) Industry and Academia; c) Intelligence analysts; d) Military and civilian researchers and practitioners interested in S&T in the cybersecurity domain; e) Experts from the ICT sector.

Collaboration and coherence with the European Defence Agency's and the NATO Science and Technology Organization's stakeholders are also identified as crucial. The CNO will closely cooperate with and support the capability efforts of all EU and NATO political and military structures and agencies and the Centres of Excellence. The collaboration environment can further expand whenever this makes a benefit for the CNO and its stakeholders.

Maintaining the network goal consensus

The prevailing perspective for collaboration in this CNO has a long-term horizon. The CNO is governed based on the Organisations' Charter – a document agreed by the founding members.

The CNO's central governing body is the General Assembly (GA) chaired on a rotational basis by each representing member. The Chair and the Vice-chair of the GA are first among equals, and the CNO members elect the Vice-chair for 2 years. After serving two years as a Vice-chair of the GA, the person becomes automatically Chair. This approach allows the Vice-chair to gain experience in managing the GA.

Each member of the CNO must be represented at the GA where the corresponding organisation has the right to nominate up to three representatives. Only one of them has voting rights.

The GA decides and approves the Mission, Vision and the Strategy of the CNO.

The management of the day-to-day business in the CNO is the responsibility of the Steering Board (SB) led by the Chair and the Vice-chair elected for two years on a rotational basis from the members of the CNO. The SB is responsible to implement the decisions of the GA. The SB exercises unified governance of the CNO by: (1) Developing and updating the long-term S&T Strategy and medium-term S&T Priorities; (2) Propose network-wide goals and documents like

CNO Operative Procedures (OPs), Collaborative Program of Work (CPoW), etc.; (3) Acting as the focal point for coordinating the CNO S&T CPoW; (4) Provision of guidance and direction for the operations of the CNO scientific-technical committees and working groups; (5) Obtaining GA approval of the S&T Strategy and medium-term S&T Priorities and plans; (6) Obtaining GA approval of the CNO's CPoW and the annual budget.

The CNO's Cooperative Programme of Work and its budget are submitted by the SB annually for GA approval.

The work of the SB is supported by the Permanent Executive Committee (PEC) acting as secretariat, and led by Chief Executive Officer (CEO) who is responsible for: (1) Appropriate administration of the CNO members in the following activities: a) Candidate-members' application review; b) Membership registering; c) Auditing and review of members' status; (2) Providing effective planning and coordination for S&T undertakings; (3) Administration and publication of CNO Collaborative Network activities, and coordination of CNO public relations matters.

The Scientific Advisory Board is a consultative body, providing its expertise to the SB and its Chair, as well as the CNO members, on knowledge, information management, and technology and policy matters to the benefit of the organisation.

There are rules in place for monitoring and auditing the goal compliance of the members, described in the CNO Operative Procedures. The SB is responsible for monitoring the goal compliance of the CNO members and it decides on the quality of CNO S&T output.

There are consequences for the participants if they do not comply with the CNO's goals and do not provide good quality of S&T products. Following the CNO's Charter and the agreement on the Articles of association of the CNO, membership to the organisation shall end if a member fails to fulfil its statutory obligations. Termination or expulsion by the CNO shall be decided by resolution of the General Assembly.

Maintaining the trust within the network

The collaboration within the CNO is a consensus-driven, and there is a tendency to achieve consensus wherever and whenever possible. Within the organisation, real progress is achieved through democratic processes. The focus is on strategic objectives that are universally shared.

This does not imply unanimity is needed on specific issues that are subordinate to the strategy (for example, deployment architectures, technology choices, or funding models), where compromise is often necessary, or where multiple approaches can be completed in parallel. If consensus is not possible to achieve, the qualified majority can be applied to all decisions at all levels of the CNO governance.

There are no weights of votes. Each member has one voting representative in the central governance and management bodies (e.g. GA and SB).

The CNO ensures that appropriate internal and external transparency rules are in place to guarantee free access of the members to strategic documents, monitoring and auditing reports. The rules are described in the CNO's Operative Procedures.

Internal Member's area information and public information are provided by the CNO Portal, Permanent Executive Committee and the internal network.

The CNO maintains a web portal dedicated to the community of cybersecurity experts - Cyber Security Research Connections. This approach provides a better opportunity for information exchange and easy networking for relevant European defence and security stakeholders for cooperation around topics of common interest.

The CNO's Annual Reports regarding the stakeholders, customers and potential member engagement are published and can be found at the organisation's web portal. Drafts of contractual documents for stakeholders describing the rights and level of engagement, as well as Multi-Beneficiary Model Grant Agreement can be found at the Portal.

In the conduct of its mission, the CNO implements approved Information assurance policies, which ensure that commercial information shared under the auspices of the CNO is duly protected by appropriate and approved by the GA Information Management Policy.

Conflict resolution procedures exist. They are described in the following documents: (1) The Charter of the CNO; (2) The CNO Association Bylaws and regulations; (3) The CNO Operative Procedures.

Centralisation and horizontal links

The organisational architecture of the CNO is based on the Central Network Hub (CNH) principle. This means that there is a Central Network Body (CNB) established which is supported by a Permanent Executive Committee. Besides, there exists a Network of National Points of Contact (NNPoC) that have an important role in the coordination of the CNO's work with the Members. The CNH and the NNPoC are the spinal columns of the organisation.

The Hub coordinates and facilitates the members' activities through the Portal and periodically held (twice per year) face-to-face meetings.

There is a high level of coordination of S&T activities through the CNO central bodies. The proposals for new activities are drafted by the Scientific Committees. After that, the proposals are reviewed, evaluated and rated by the Knowledge and Information Management Committee and endorsed by the SB. The GA makes the final decision on the proposals twice per year and they become part of the CPoW.

The CNO members work together to provide network connectivity and to collaborate on joint S&T activities, investing in the development and delivery of an advanced portfolio of services, tools and network capabilities to institutions, projects, researchers and policy-makers in Europe and worldwide.

The participants in the CNO can decide to collaborate on their projects. At least four CNO members have to express interest and to allocate resources for

S&T cooperation to initiate a new activity. There is no requirement for all other participants to join this activity. After endorsement by the SB and approval by the GA, the new activity can start. The rules for cooperation are described in the Operative Procedures of the CNO.

The SB, with the support of the Permanent Executive Committee, exercises the oversight on the implementation of the S&T activities and reports to the GA twice per year about the implementation of the CPoW.

Network Competences and Certification Procedure

The use of standards and information from standardisation bodies are of great importance to and continue to be incorporated in the development of CNO's services to ensure interoperability with services of other relevant collaborative networked organisations.

The CNO is highly active in guiding and influencing international standards development – ensuring interoperability across the research and education community in the cybersecurity domain. There are the Scientific Advisory Board and Certification Commission established. Both structures are responsible for CNO's competencies monitoring and guaranteeing standardisation procedures implementation.

The CNO influences standards development through participants making significant contributions in Open Grid Forum, Internet Engineering Task Force Standards Organisations and the European Standards Organisation.

There is a procedure in place for monitoring and auditing of competences in the framework of the CNO. They are described in the Charter and the Operative Procedures of the organisation. The CNO Steering Board is responsible for internal auditing, while professional auditing is yearly, and external experts do it.

Risk Management and Shared Funds

The CNO has agreed among the participants and approved by the GA Rules for risk identification, management, and monitoring. It is the responsibility of the SB to prepare and to submit for approval by the GA the Risk Management Strategy. The Rules and the Strategy are reviewed and updated regularly by the SB according to the needs of the organisation, the changing environment in which the CNO operates and the foreseen risks and security posture. The CNO does not allocate centrally reserve funds for risk events.

The main document, which governs the CNO's financial and budgetary affairs, is the Organisation's Financial Regulations (FR). The responsibility of the Budget Committee is to develop the FR of the CNO and to present them for endorsement by the SB. After that, the Regulations have to be approved by the GA.

According to the Charter, the CNO operates within the financial budget set annually by the General Assembly. The Budget Committee, acting by a qualified majority, adopts the draft yearly budget. When doing so, it should suggest the Steering Board to review and endorse the budget. Finally, the GA approves the proposed yearly budget.

The CNO's budget is funded by several sources: (1) The European Union's research and innovation programmes; (2) The CNO members are required to pay an annual membership fee to be determined by the General Assembly. All members will pay the same membership fee; (3) some members shall be customer-funded after approval by the GA; (4) Ad-hoc projects or programmes and budgets funds from additional revenue.

The General Assembly can decide to compensate some CNO members and reimburse their expenses. The Chair of the SB may transfer money between CNO's accounts without limit, after approval by the GA.

According to its Charter, the International Board of Auditors (IBA) acting on behalf of the GA, shall audit the financial statements of the organisation. The IBA may carry out performance audits that shall ascertain that the operations of the CNO have been implemented in compliance with economy, effectiveness and efficiency principles. The IBA shall have access to any information necessary to conduct its financial and performance audits.

The Steering Board, acting on a proposal from the CEO, shall as necessary adopt the rules regarding the implementation and control of the general budget, notably as regards public procurement. The Steering Board shall ensure, in particular, that security of supply and protection both of defence secret and intellectual property rights requirements are duly taken into account.

Conclusions

The governance model of a CNO for cybersecurity research presented in this paper is oriented towards the mission to enable collaboration among EU MS, NATO and the partner Nations of the two Alliances to improve cybersecurity capabilities, particularly in the S&T domain.

Once again, this is not an existing governance model. Instead, it is an abstraction aiming at suggesting one possible option on how to govern and manage such a complex organisation. The goal of this exercise was to support the process of identification and selection of the future governance model of the ECHO network suggesting one possible option.

We are fully aware that the EU Regulation 630 gives preference to the development of a Cybersecurity competence network with a dual mandate to pursue measures in support of industrial technologies as well as in the domain of research and innovation, not a separate network focused on S&T activities only. Our idea is just to emphasize the importance of cybersecurity S&T domain as one of the most important undertakings of the future ECHO CNO.

The final preference for the ECHO network governance model selection will be made after completion of a comprehensive analysis. Currently, the research team is applying the Analytical Hierarchy Process methodology to analyse the evaluation of subject matter experts on the formulated four alternative governance models described in the introduction of this paper. The goal is to identify which of these alternatives will better serve the ECHO network. This process goes in parallel with the governance needs and objectives assessment for the establishment of a CNO in the area of cybersecurity.[21]

Most probably the future ECHO governance model will include both a central governance body and regional (or sectoral) centres bringing together academia, industry, cybersecurity practitioners and end-users. This approach should guarantee integration of ECHO CNO in the future EU cybersecurity landscape as regards the EU Regulation 630 for establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres.

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 author gratefully acknowledges the contribution to the primary analysis of Collaborative Network Organisations by Mr Georgi Ganev.

References

1 "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions," Brussels: European Commission, High Representative of the European Union for Foreign Affairs and Security Policy, 2013, p. 20.

2 European Commission, "Proposal for a 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," Brussels, 12.9.2018 COM(2018) 630 final 2018/0328 (COD).

3 European network of Cybersecurity centres and competence Hub for innovation and Operations (ECHO), available from https://echonetwork.eu/, accessed on 20.04.2020.

4 Yantsislav Yanakiev and Todor Tagarev, "Governance Model of a Cybersecurity Network: Best Practices in the Academic Literature," In: *Proceedings of ACM International Conference on Computer Systems and Technologies (CompSysTech'20)* (New York, NY, USA, ACM, 2020), https://doi.org/10.1145/3407982.3407992.

5 Dirk Hovorka and Kai Larsen, "Enabling Agile Adoption Practices through Network Organizations," *European Journal of Information Systems* 15, no. 2 (2006): 159–168.

6 Francesca Grippa, João Leitão, Julia Gluesing, Ken Riopelle, and Peter Gloor, *Collaborative Innovation Networks: Building Adaptive and Resilient Organizations* (Cham, Switzerland: Springer, 2018).

7 Amanda Abreu and João M.F. Calado, "Risk Model to Support the Governance of Collaborative Ecosystems," *IFAC Papers OnLine* 50 (2017): 10544–10549.

8 Todor Tagarev and Brid Davis, "Towards the Design of a Cybersecurity Competence Network: Findings from the Analysis of Existing Networks," *10th International Conference on Multimedia Communications, Services & Security (MCSS 2020),* Krakow, Poland, October 2020.

[9] NATO Science & Technology Organization's Collaborative Program of Work (CPoW) 2019.

[10] Chapter of the Science and Technology Organization (STO), 1st July 2012, Available at https://www.sto.nato.int/Pages/sto-panels.aspx, accessed on 1.04.2020.

[11] NATO Science & Technology Organization's (STO) CPoW Operating Procedures, 2019.

[12] Chapter of the Science and Technology Organization.

[13] GÉANT Bylaws, available at https://www.geant.org/About/Our_organisation/Documents/GA(15)034r2-Bylaws-20160418.pdf, accessed on 01.04.2020.

[14] GÉANT Strategy 2020, Implementing the Strategy, Available at www.geant.org/Resources/Documents/Strategy2020_Over-the-Horizon.pdf.

[15] GÉANT Bylaws.

[16] Council Decision (CFSP) 2015/1835 of 12 October 2015 defining the statute, seat and operational rules of the European Defence Agency.

[17] Council Decision (EU) 2016/1351 of 4 August 2016 concerning the Staff Regulations of the European Defence Agency.

[18] Council Decision (CFSP) 2015/1835.

[19] Council Decision (EU) 2016/1353 of 4 August 2016 concerning the financial rules of the European Defence Agency.

[20] Andrea Cardoni, Stefano Saetta, and Lorenzo Tiacci, "Evaluating How Potential Pool of Partners Can Join Together in Different Types of Long Term Collaborative Networked Organizations," In: L.M. Camarinha-Matos, X. Boucher, and H. Afsarmanesh (eds.), *Collaborative Networks for a Sustainable World, PRO-VE 2010, IFIP Advances in Information and Communication Technology*, vol. 336 (Berlin, Heidelberg: Springer, 2010), pp. 312-321.

[21] Todor Tagarev, "Towards the Design of a Collaborative Cybersecurity Networked Organisation: Identification and Prioritisation of Governance Needs and Objectives," *Future Internet 12,* no. 4 (2020): 62, https://doi.org/10.3390/fi12040062.

About the Author

Captain (BGR-N) (ret.) Yantsislav **Yanakiev** is a full professor in sociology at the Bulgarian Defence Institute "Prof. Tsvetan Lazarov." He specialised as an International Research Fellow at the NATO Defense College in Rome, Italy Cologne University, Germany, and George C. Marshall Centre for International Security Studies. Prof. Yanakiev was a Fulbright Senior Visiting Researcher at the Defense Equal Opportunity Management Institute, Patrick Air Force Base, FL, US. He has been the principal national representative to the NATO Science and Technology Organization, Human Factors and Medicine Panel since 2005 and he was bestowed an Individual Scientific Achievement Award of the NATO Science and Technology Organization for 2018. https://orcid.org/0000-0003-0664-1661