Collaborative Cybersecurity Networked Organisations

Subjects: Computer Science, Information Systems | Management | Business
Contributor: Todor Tagarev

The requirements to the governance of collaborative networked organisations (CNOs) can be structured in 33 categories: Geographical Representation or exclusion; Supply chain security; Involvement of external stakeholders; Standards and methodologies; Representation on senior governance bodies; Decision making principles; Auditing; Dispute/conflict management arrangements; Confidentiality & Security; IPR management; Ethics code; Use of slave labour or labour of minors; Green policies; Gender policies and representation; Transparency; Accountability ; Anti-corruption/ integrity policies; Innovation; Adaptiveness; Cohesion; Trust; Sustainability; Resilience; Communication and engagement; Knowledge management; Long-term perspective on collaboration; Interoperability; Leadership; Organisational culture; Competences; Risk management; Evidence-based decision-making; and Competitiveness.

As a result of a comprehensive study for CNOs in the field of cybersecurity these governance issues have been structured in two groups (of governance objectives and CNO features) and four tiers in terms of priority. While the governance categories are universally applicable, their prioritisation is relevant for CNOs in the field of cybersecurity.

Keywords: collaborative networled organisation ; governance ; cybersecurity

1. Introduction

Modern societies increasingly rely on information and communications technologies and infrastructures in their economies, the provision of public services, and social interaction. While access to abundant information and digital infrastructures provide various advantages, they introduce vulnerabilities that are readily exploited by malicious actors in the pursuit of financial gain, i.e., through cybercrime, or political objectives by gathering intelligence, retaliation against an attack, disrupting essential services during conflict, interfering in elections, and other forms of cyber warfare and cyber terrorism [1]. Accordingly, information and cyber security incidents have evolved from isolated attacks to targeted, sophisticated cyber threats at individual, organisational and even national levels [2].

Notwithstanding the risks of malicious exploitation, advanced sensors, actuators, computational technologies, increased data storage, communications, achievements in artificial intelligence, etc., will be progressively incorporated in industrial processes, transport vehicles and networks, health services, critical infrastructures and homes. The provision of safety, security and privacy in utilising the benefits of technology will remain a persistent challenge in the foreseeable future [3].
Very few organisations have the resources and the competencies required to protect their communications, information systems, and smart devices from attacks through cyberspace. In fact, only a few countries have the resources to develop and deploy autonomously technological and organisational solutions to counter effectively the threats from cyberspace.

The European Union as a whole looks for creating a reliable, safe, and open cyber ecosystem through enhanced networking and collaboration between Member States and EU agencies, public and private actors, academic organisations and industry. By establishing a collaborative network, participating organisations expect to get access to competencies and/or resources complementing their own and thus to access new markets and meet emerging demands from public authorities and industry while sharing risks with partners. The advantages of collaborative arrangements are numerous; yet, their proper exploitation requires the establishment adequate governance.

2. Development

To identify and prioritise governance requirements, a dedicated study used four types of information sources: norms and regulations; existing networked organisations; academic publications; and interviews with stakeholders. 33 categories of governance issues were identified on that basis. They were split in two groups:

- Those that can be designated as “objectives” which can be achieved by devising and effectively implementing sets of normative, organisational, procedural, technical and training measures (included in the second column of the table

below);
- Those that depend on various intangibles and the interplay of numerous factors and contexts, and can be addressed only partially by norms, procedures, training and technical measures. These governance issues are designated as “features of CNOs” and included in the third column of the table),

And classified in tiers depending on the number of times they have been addressed in primary sources (with Tier 1 including issues of highest interest, hence possibly of highest priority; followed by Tier 2, etc.).

Tier	Governance Objectives	Features of CNOs
1	Geographical representation or exclusion; Involving external stakeholders; Representation; Decision making; Auditing; Confidentiality and Security; Knowledge management; Standards and methodologies; Long-term perspective on collaboration; Competences; Risk management; Evidence-based decision-making	Adaptiveness; Cohesion; Trust; Competitiveness
2	Supply chain security; Dispute/conflict management arrangements; Intellectual Property management; Ethics code; Gender policies and representation; Transparency; Accountability; Integrity/anti-corruption policy	Innovation; Leadership
3	Communication and engagement	Organisational culture; Sustainability
4	‘Green’ policies; Slave labour, labour of minors; Interoperability	Resilience

The list of governance issues is currently used to inform the development of alternative governance models and a weighted set of criteria for their evaluation, and hence to make an informed decision on the most appropriate governance model (or models) for the future cybersecurity network.

References

1. Goel, S. National Cyber Security Strategy and the Emergence of Strong Digital Borders. Connect. Quart. J. 2020, 19.
2. L. O. Gontar’; Legal procuring of international information/cyber security of the digital economy: economic and legal aspects. *E-Management* **2019**, , 61-66, 10.26425/2658-3445-2018-2-61-66.
3. Jatinder Singh; Christopher Millard; Chris Reed; Jennifer Cobbe; Jon Crowcroft; Accountability in the IoT: Systems, Law, and Ways Forward. *Computer* **2018**, *51*, 54-65, 10.1109/mc.2018.3011052.