future internet

MDPI

Article

Towards the Design of a Collaborative Cybersecurity Networked Organisation: Identification and Prioritisation of Governance Needs and Objectives

Todor Tagarev

Institute of Information and Communication Technologies, Bulgarian Academy of Sciences, 1113 Sofia, Bulgaria; tagarev@bas.bg

Received: 10 March 2020; Accepted: 27 March 2020; Published: 28 March 2020

Abstract: The effective response to the proliferation and growing diversity and sophistication of cyber threats requires a broad spectrum of competencies, human, technological and financial resources that are in the powers of very few countries. The European Union is addressing this challenge through an initiative to establish one or more cybersecurity competence networks. A number of existing technologies can support collaboration in networked organisations; however, network governance remains a challenge. The study presented in this article aimed to identify and prioritise network governance issues. Towards that purpose, qualitative and quantitative methods were applied in the analysis of norms and regulations, statutory documents of existing networks, academic sources and interviews with representatives of funding organisations and potential major customers. The comprehensiveness and complementarity of these primary sources allowed to identify 33 categories of governance issues and group them in four tiers, indicative of the respective priority level. The results of the study are currently used to inform and orient the development of alternative models for governance of a cybersecurity network and a set of criteria for their evaluation. They will support informed decision-making on the most appropriate governance model of a future networked organisation, evolving from a project consortium.

Keywords: cybersecurity competence network; collaborative networked organisation; network governance; requirements; prioritisation

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. A recent

study on organising national cybersecurity concluded that one of the main choices is whether to centralise cyber capacity in one unit or spread it across different sectors [4]. Government agencies of countries like Belgium and Bulgaria recognise in their strategies that, as cyber threats become more complex, there is a growing need to expand horizontal coordination [5] and engage with multiple stakeholders, including those from industry and academia [6]. 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. The European Parliament and the Council issued in 2018 a proposal for a Regulation on establishing a European cybersecurity industrial, technology and research competence centre and a network of national coordination centres [7]. A call for proposals within Horizon 2020 was issued in parallel with the goal to overcome the fragmentation of EU research capacities and ensure that "the EU retains and develops essential capacities to secure its digital economy, infrastructures, society, and democracy" [8]. More specifically, the call aimed to establish and operate a pilot for a "Cybersecurity Competence Network," and four such pilots, selected in a competitive procedure, were launched in 2019.

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 in manufacturing have been exploited for at least two decades and since mid-2010s became subject of rigorous study [9]. This trend is relatively new for the field of cybersecurity. Nevertheless, it has already attracted considerable attention.

Expectedly for such high-technology field, researchers already explore the benefits of advanced technological solutions such as blockchain [10,11] and translation gateways [12] to support collaborative processes. Others focus on developing ICT architectures encompassing numerous security layers [13] and integrating a number of frameworks, models and methodologies [14], with a particular interest in service-oriented architectures and their use to support governance of collaborating enterprises [15]. Another example of the technical perspective on collaboration is the application of the concept of System of Systems to study collaborative organisations, their behaviour and performance [16]. The implementation of best practices and standards complements the studies of cybersecurity, in particular in relation to the Internet-of-Things (IoT) and the concept of Industry 4.0 [14,17].

While some of the referenced sources claim that the technical solutions offered help solve issues related to interoperability, collaboration, security, and value chain governance [10,11], the problem with the governance of collaboration persists. Some authors go as far as to designate the exclusive reliance on technological solutions as "libertarian techno-utopianism" [18]. The IoT is of particular concern. While the IoT has facilitated automation of industrial processes, transport and homes, its rapid growth is also a cause for significant security and privacy concerns due to the absence of effective regulation, standards and weak governance [19].

The increasing reliance on private providers of cybersecurity services is also a cause of concern. That includes the quasi-governmental role of the private actors on key cybersecurity issues [20] and known cases of security breaches and access to sensitive data of non-vetted foreign private employees [21]. The public–private governance of critical information infrastructures is just one example of the existence of an accountability gap, i.e., a gap in governance [21]. Other studies of connected systems and organisations also demonstrate that "the management of safety and security risks ... requires the extension of existing governance mechanisms, including regulation, standards, and industry best practices, to combine both safety and cybersecurity" considerations [22], as well as understanding shared risks [23].

Some of the governance aspects of collaboration have already been addressed, demonstrating that:

- the effective contribution of private persons to formal computer emergency response arrangements, e.g., crowdsourcing, requires recognition and division based on the roles and individual needs and can encourage 'netizens' to co-produce cybersecurity [24];
- trust is key for sharing cyber intelligence and motivating partners to join a cybersecurity alliance [25];
- the timely identification, management and resolution of conflicts among partner organisations is key for successful collaboration [26];
- traditional assessments of security risks often focus on tangible assets, while intangibles such as tacit knowledge are in some cases more important than physical assets [27];
- knowledge sharing is a fundamental factor for strategic decision making, particularly in relation to innovation management and sustainability of collaborative organisations [28];
- Interoperability is a must for cybersecurity information sharing and timely threat intelligence [29].

This partial list provides just a glimpse into the governance challenges of cybersecurity collaboration. The challenge is much more extensive, which explains why policy-governed (and not technology-driven) and secure collaboration is defined by the Science of Security initiative of the US National Security Agency as one of the top five 'hard problems' of cybersecurity [30].

One of the four pilot projects launched to establish a cybersecurity competence network on the basis of the project consortium includes 30 partners from 14 European countries [31]. Recognising that networks differ widely in terms of history, activities, communication modalities, member commitment, consensus on goals, perceptions of results, and respective governance structures [32], the project invests significant effort into designing, implementing and enhancing an adequate network governance model.

The first stage of the design was to identify and prioritise governance needs, objectives, and requirements. This article presents the results of the respective study, that led to the identification of 33 categories of governance issues grouped in four tiers in terms of priority. The prioritised list, along with best practices in business and governance models of collaborative networked organisations, serves in the next stage of the study both to design and to evaluate alternative governance models and select the most appropriate model for governing a future cybersecurity competence network evolving from the project consortium.

2. Materials and Methods

Collaborative networks consist 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" [9]. Subject of this study is the governance of Collaborative Networked Organisations (CNOs) consisting of independent organisations, connected by IT, that work together to jointly accomplish tasks, reach common goals and serve customers over a period of time [33]. In the study's working definition of governance, the term is defined as *specification of rules, criteria for decision-making, responsibilities, and boundaries of actions and autonomy for the actors involved in the CNO* [34].

The study of governance of cybersecurity requires interdisciplinary research [30] drawing, among others, from governance theory, actor-network theory, and the study of sociotechnical regimes [35]. Research on Internet governance has already utilised actor-network theory and interpretative policy analysis to conceptualise multi-stakeholder arrangements engaging heterogeneous actors [36,37]. The study of governance challenges and models in another one of the four pilot projects also utilises actor-network theory and is based primarily on interviews with stakeholders [38].

This study used four types of information sources: norms and regulations; existing networked organisations; academic publications; and interviews with stakeholders. It was organised in four phases: (1) Preparation; (2) Preliminary analysis; (3) Secondary analysis; and (4) Aggregation.

In the *Preparation* phase, based on analysis of the project documents, own experience and an online search, a core team of researchers prepared a list of governance issues, issues related to business and governance models of networked organisations and a list of existing organisations of possible interest, and distributed them among partners for feedback and amendment. An amended draft was discussed during a project meeting, leading to a final draft list and a template in Excel format to present the analysis of networked organisations. The template was piloted by six partner organisations, analysing 12 networks in total. The feedback received from piloting the template and the overall analysis process was used to prepare the final template. The list of governance issues in this final template served also to construct the questionnaire for interviews with stakeholders (which included an additional open question) and to orient the selection and analysis of normative documents and academic sources.

In the second phase of the *Preliminary analysis,* partners analysed three types of sources in parallel:

- Ninety-two existing network organisations of four kinds: networks dedicated to information/cybersecurity research and services; cybersecurity incubators/accelerators/tech parks/ecosystems; other research-intensive networks; and networked organisations providing (among others) information services related to cybersecurity (for the full list of the analysed network organisations see Supplementary S1);
- Fourteen regulations and other normative documents, related to the governance of networked organisations in the field of cybersecurity, including relevant EU norms and available governance documents of the four pilot projects;
- Sixty academic articles, books, book chapters and conference papers. In the identification of sources, an initial list of 543 publications was generated by a Scopus search for "networked organizations"/"networked organisations" AND "collaborative". A subset was selected by reviewing abstracts to identify sources discussing governance issues. In addition, preference was given to more recent and open-access publications, adding also books presenting comparative analyses and benchmarking studies of collaborative networked organisations (for the full list of the analysed academic sources see Supplementary S2).

The fourth source of information came from conducting interviews with stakeholders. Nine person-to-person interviews were conducted. Three of the interviewees represented funding organisations (including one current and one former national cybersecurity coordinator), while the other six were mid- to senior-level representatives of potential major customer organisations. The interviewees came from seven EU Member States and two represented the views of EU-based international organisations. Researchers transcribed the interviews and translated them into English.

In the phase of *Secondary analysis*, the results of the preliminary analysis for each type of primary source—extracts from normative documents and academic sources, bylaws of existing networked organisations, and interview transcripts—were processed using both qualitative and quantitative analysis [39,40]. Content analysis was used to highlight issues of interest and group them in categories of governance issues (needs, objectives, requirements). Then, the information on each primary source was coded vis-à-vis each governance issue/category, i.e., assigning "1" if the governance issue is referenced in the text or the interviewee considers it important, or "0" if it is not or the interviewee sees it as not sufficiently important to comment. The same coding method was applied to excerpts from normative documents, academic publications, and documents of existing networks.

For each type of primary source, a maximum was defined, equal to the highest number of primary sources addressing a certain governance issue. Then, the interval between 0 and the maximum was split in quartiles. All governance categories were placed in four tiers, with Tier 1 including issues of highest interest, hence possibly of highest priority; followed by Tier 2, etc.

The final phase of *Aggregation* of results from various sources allowed to highlight the key issues in business and governance models of network organisations and, in particular, to prioritise governance needs, objectives, and requirements. Each governance issue was placed in the highest tier it appears in

in the secondary analysis, i.e., even if in the secondary analysis it appears only once in Tier 1, it was placed in the highest priority tier as a result of aggregation.

This approach was adopted to reflect on the complementarity of the primary sources. For example, so far, the academic literature on governance of collaborative networked organisations practically does not treat networked organisations in the field of cybersecurity (which are still emerging) and hence the respective secondary analysis places confidentiality and security in Tier 4. When, however, cybersecurity is the focus, e.g., in the interviews with stakeholders and in the analysed norms and regulations, it is placed in Tier 1.

3. Results

This section presents results from the secondary analysis by type of primary source and concludes by aggregating these results and prioritising governance needs and requirements. All governance categories are listed consecutively with a number in parentheses.

3.1. Analysis of Interviews

This sub-section presents briefly results from the secondary analysis of transcripts of the interviews with stakeholders (fuller description is provided in [41]). It starts with the responses along the 16 governance issues included in the questionnaire, then presents an analysis of the responses to the open-ended invitation to address additional governance issues, and concludes by ranking the governance issues based on the stakeholders' views.

Profit Orientation

The first question was whether profit or non-profit arrangements are preferable for a cybersecurity network. All interviewees considered both options possible. Two of them gave some preference to non-profit arrangements citing as reasons that it would be easier to reach an agreement between member organisations and to exercise public oversight. Another two of the interviewees would prefer for-profit arrangements that would provide better opportunities for investing in CNO capabilities and infrastructure. A fifth interviewee combined the two types of arguments, stating that non-profit organisations may be selected for some funding streams, while for-profit arrangements might be preferable in terms of sustainability of the network.

This is interpreted as de facto agreement that, while the profit orientation is important for the CNO business model and the respective governance model, it is not a governance issue per se and was not included in further considerations as such.

(1) Geographical Representation or Exclusion

One interviewee noted that the composition of the network depends on its purpose, and this is reflected in all responses. Two focused on national representation; one of them stating that "national arrangements are preferred for strategic sectors [as cybersecurity]". Most interviewees stated that balanced, EU-wide representation is necessary or even crucial. One emphasised the need to achieve cohesion by providing support to less developed regions, e.g., by a strategy of smart specialization; another interviewee stressed that EU cohesion is important to guarantee "European cyber sovereignty". Two of the responses addressed local representation as beneficial, but not mandatory in one case, and as advantageous in competing on target (local) markets in the other. One interviewee stated that an EU-centred network should be flexible to include partners also from both EU-associated and NATO countries. Two of the respondents stated that EU-centred networks cannot be open to partners from "Eastern countries".

(2) Supply Chain Security

The question of involving non-EU partners relates to supply chain security concerns. The majority of the respondents shared these concerns, while the provision of skills (both basic and advanced) and

of R&D capacity, in particular R&D in academia, was noted. The views on supply chain security measures differed widely—from preference for a completely national management of cybersecurity services or at least a requirement for national security accreditation through the need for complete tracking of the supply chain (understanding that "advanced social engineering and the chain of supplies are extraordinarily good tools to violate a system") to a view that having in place legally binding agreements is sufficient.

(3) Involvement of External Stakeholders

All interviewees agreed that a network organisation should involve external stakeholders and identified several possible roles and modalities. The views on involving governments differ. Two interviewees stated that governmental (political) stakeholders need to be involved, while one asserted that "representation [on network bodies] of organisations with political or governmental affiliation should be avoided".

(4) Standards and Methodologies

The interviewees identified a number of norms, frameworks, and methodologies to be followed, and one of them stressed the need to adopt a standards-oriented approach to network governance and management. However, in their responses, most interviewees did not focus on standards and methodologies, but emphasised instead that the governance model needs to provide for flexibility of the decision-making process and autonomy in implementation, including giving the "right level" of autonomy to the CEO in the decision process, unity of purpose of the network and capacity to adapt to changing circumstances. One interviewee pointed to the need to have rules and procedures in place to allow for processing sensitive information and, in certain cases, of classified information.

(5) Representation on Senior Governance body/Ies

All interviewees who responded to this question stated that "fair" representation of network members on the senior governance body or bodies is sine qua non, a factor that will influence decisions on using the services provided by the network or not. Some more specific points were made regarding regional representation, representation of EU member states plus key agencies, and the need to provide for collaboration between academia, industry and government.

(6) Decision Making

Interviewees agreed that consensus is the preferred desired decision-making principle, but may be difficult to reach. Yet, decisions on some issues, e.g., adding a new partner to the network, need to be taken by consensus. On other issues, decisions can be taken by a majority vote. The opinions of interviewees who commented on this are equally split—some consider simple majority sufficient, while others call for decision-making by qualified majority.

(7) Auditing

One third of the interviewees dismissed the question on the need for internal and/or external audits. The remaining respondents agree that regular auditing is necessary. There is preference on using external auditors, that are not (and have not been) part of the network operation. One interviewee emphasised that the external auditors need to have a mandate; for an "EU network" this mandate should be given by a respective EU organisation.

(8) Dispute/Conflict Management Arrangements

Two thirds of the interviewees consider that it is important to have some sort of arbitration in place to resolve disputes or conflicts between partners in the network and a number of modalities were suggested. Respective rules need to be set in advance.

(9) Confidentiality

Most interviewees refer to confidentiality as a crucial consideration for the proper functioning of a network organisation in the field of cybersecurity, including the protection of personal data and other sensitive or classified information, and suggested a number of specific measures.

(10) Intellectual Property Management Arrangements

Most interviewees saw intellectual property management arrangements as needed or very important, e.g., to protect valuable knowledge, competence and capacity while facilitating collaboration and sharing of experience. One interviewee advised to follow the European Commission rules for the IPR developed under EU funding, but introduce specific arrangements for customer funding, and in all cases to seek preservation of IPR for the network organisation, thus allowing to multiply to results of the common work.

(11) Ethics Code

Nearly half of the interviewees consider ethical behaviour as an issue that does not require special discussion, since all network partners are expected to adhere to applicable EU policies and guidelines. Yet, other respondents state that a network organisation needs an Ethics Code and outlined its purpose and key content.

(12) Specific Ethical Issues

The interviewees were asked to evaluate the relevance to cybersecurity networks of specific ethical issues, such as policy in regard to *slavery* and the use of *labour of minors* in the supply chain. Most respondents consider these issues either not applicable or not in need of discussion. The general opinion is that adherence to the relevant EU regulations and guidelines will suffice in this respect.

(13) 'Green' Policies

Most interviewees agree that environmental considerations are important, but they cannot be in the focus of network governance policies and models, and that adherence to "applicable EU policy" is sufficient.

(14) Gender Policies and Representation

Just over half of the interviewees elaborate on this governance aspect, some clearly stating that this is "not a fundamental aspect; [we need to] put the merit in front of gender equality". Others are content with adherence to "applicable EU policy". One of the interviewees recommended adopting an "equal treatment, equal opportunities" framework.

(15) Transparency

Transparency of network governance is seen as sine qua non by more than half of the respondents. One of the respondents stated: "We enter only networks that are transparent to participants and respect the integrity of network partners".

(16) Accountability

Half of the interviewees see accountability also as an essential prerequisite that can be guaranteed, for example, by introducing requirements for publication of an annual report and a financial statement, separation of roles and responsibilities to make sure that decision-making bodies abide to transparency requirements, and assuring compliance to the regulatory, legal and operational framework defined in the founding charter of the network.

(17) Anti-Corruption/Integrity Policies

Interviewees were asked to assess the importance of other good governance issues, including integrity, protection of whistleblowers, or anti-corruption policy more generally. More than half of them considered these aspects important, and one called for "maximum transparency and integrity in the governance." The general view, however, is that if one follows EU legislation, no special additional requirements need to be set. One specific recommendation was to provide "special training [for network organisations' personnel] for conflict of interest and anti-fraud, plus e-exam and signing of a declaration".

Table 1 presents the prioritisation of these 17 governance issues on the basis of the responses to the interviews.

Table 1. Stakeholders' views on cybersecurity network governance.

Tier	Governance Categories
1	Geographic representation; involvement of external stakeholders; decision-making arrangements; confidentiality
2	Supply chain security; representation on the senior governance bodies; auditing; dispute and IPR management; Ethics code; gender policy; transparency, accountability and integrity
3	Standards and methodologies
4	Use of slave labour or labour of minors; 'green' policies

The responses to the open question reconfirmed the importance of ethical considerations, transparency, openness and accountability, and highlighted in addition:

- the importance of achieving and maintaining trust between the partners and to the network as a whole;
- network's cohesion;
- knowledge sharing;
- the need to introduce results-oriented management, supported by appropriate instruments for performance monitoring and measurement, e-Procurement, and provision of information and targeted training opportunities;
- quality control;
- resiliency and sustainability of the network;
- the role of strategic communication and engagement.

3.2. Network Governance Issues in Academic Sources

Sixty articles, conference papers, books, and book chapters were analysed to identify the best practices in setting up business and governance models of collaborative networked organisations and elicit additional views on network governance issues. This subsection presents the results on the latter objective, reflecting also interviewees' responses to the open question, grouped in another 16 governance categories.

(18) Innovation

The need for and the opportunities for innovation provided by collaboration are addressed in 24 of the analysed academic sources. The references span from the importance of innovation to capturing new business opportunities, through the need to develop capacity and readiness to innovate, and the application of the Open Innovation paradigm arguing for the need to establish new models, where much of the knowledge comes from outside the boundaries of the company [42], to the call for establishing Collaborative Innovation Networks, or COINs—"self-organizing emergent social systems"—as "primary building blocks of innovation" [43].

(19) Adaptiveness

Based on the analysis of the academic literature, adaptiveness emerged as the most salient governance issue, along with the consideration of competitiveness. It is addressed by 35, or nearly 60 percent, of the analysed sources. Authors emphasise that "systems that want to live long must co-evolve with their environment" [44] and highlight various aspects of adaptiveness, including:

- CNOs' adaptability to changing environment (markets, technologies), the need to cope with external change through an adequate rate of adaptation, and evolutionary development, aiming at continuous improvement;
- flexibility and the need to swiftly adjust to market challenges and adapt to turbulent contexts;
- change management; redesign, reengineering, renewal and restructuring; process reengineering and having flexible business processes;
- agility and the capabilities "to sense and respond to predictable and unpredictable events [45];
- the capacity to self-organise, self-adapt, and exhibit emergent behaviour [16];
- achieving "strategic flexibility" [46], e.g., through adaptive policy-making [47].

(20) Cohesion

Sixteen academic sources underline the importance of achieving cohesion. Network cohesion builds on shared understanding and attitudes, negotiation and agreement on rules of cooperation, a planning and prediction process shaped by negotiation, a good level of alignment among the value systems of the various members of the network, and other intangible elements, such as reputation, friendship, interdependence, and trust. When there is harmonisation among CNO partners and cohesion of the network, one witnesses a better sense of identity, high levels of solidarity, shared passion and motivation, and better opportunities for:

- balancing interests;
- complementarity and subdivision of successes and risks;
- developing social capital;
- alignment and integration across an increasingly complex network of multiple partners and collaborators;
- exploiting creative synergies.

(21) Trust

Twenty-seven of the analysed academic sources refer to trust. Twenty-six of them look into trust among partners, i.e., trust building and confidence among participants, while five reference trust into the collaborative networked organisation by external stakeholders, users, and society, including criticality of relationships and knowledge, image and reputation of the CNO and customer confidence. Four of the sources address both internal and external aspects of trust.

(22) Sustainability

Seven of the academic sources reference aspects of sustainability, including sustenance under uncertain and rapidly changing conditions [48], that would provide for more predictable organisational behaviour and less turbulence [49], stability and robustness.

(23) Resilience

The resilience of networked organisations is referenced in six sources. A resilient organisation preserves its key functionalities under negative impact and has a capacity to recover from disruptive and even catastrophic events by securing access to critical resources and information in an effective and timely manner [50].

(24) Communication and Engagement

Eighteen of the studied academic sources address the issue of communication is several aspects. First, communication among partners in the networked organisation, in particular that related to knowledge sharing, is seen as an indicator of the level of maturity of the network [48]. Second is the communication with external stakeholders, more specifically the interaction with customers and customer communities, e.g., to receive feedback from users. Third, open and transparent communication and engagement of users and wider society may be of a strategic nature, leading to co-creation [51] and co-innovation, or "open innovation" [52]. It needs to include rewarding mechanisms for involved customers and will thus reinforce the network's social influence and support knowledge transfer.

(25) Knowledge Management

Fifty percent of the studied academic sources (the third highest percentage) emphasise the importance of knowledge management, including:

- knowledge acquisition and the organisation's capacity to transform information gathered from a vast array of diverse sources into useful knowledge;
- knowledge exchange or knowledge sharing;
- knowledge enrichment and the creation of transdisciplinary knowledge;
- knowledge representation;
- the use of knowledge (enterprise knowledge resources), e.g., for making effective decisions;
- knowledge retention or minimising knowledge loss in changes in the networked organisation.

The analysis of the literature allows also to highlight also some more specific issues of interest, such as:

- managing tacit knowledge [46,53];
- the importance of aligning knowledge management with structured business processes [53];
- the need for systematic efforts to increase the absorptive capacity of the networked organisation, i.e., its "ability to acquire, assimilate, transform and exploit new knowledge" [54];
- the conditions of performance, creativity and collaboration of knowledge workers, seen as central to an organisation's success [53];
- information and knowledge brokering and the roles a knowledge broker may play in a networked organisation [55];
- the use of active knowledge models [56].

(26) Long-Term Perspective on Collaboration

Fourteen sources, or nearly a quarter of the ones under study, refer to the need for a longer-term view on collaboration. Some of the authors emphasise prerequisites, such as having a common purpose, or coherence of the purposes of collaborating partners, and shared goals. Among the tools for achieving such a long-term perspective are the collaborative predicting and planning [57] and setting reasonable expectation of success [58]. Of particular importance is the 'strategic approach' to collaboration by establishing a long-term "network vision" [59,60] to define the strategic mission and strategic options. In that respect, some authors call for strategy-based governance and management and focusing efforts by aligning proactive strategies [61].

(27) Interoperability

The issue of interoperability is subject of discussion in seven academic sources. Some of them examine technical aspects, such as requirements to the technical infrastructure supporting the

collaboration, including requirements to information systems [16] and architecture frameworks that can be used to facilitate interoperability, while others refer to norms, procedures and allocation of decision-making roles to allow for smooth interoperation among network partners. Importantly, interoperability is included among key issues examined in assessing the readiness of collaborative networked organisations to effectively deliver their products and services [62].

(28) Leadership

Six of the examined sources refer to the leadership in collaborative organisations, including commitment, motivating and empowering members of the networks, e.g., through the enhancement of their capacities, readiness of executives able to allocate resources when needed, and adhering to the principle of neutrality in network management. Some of the authors emphasise even less-tangible aspects of leadership, such as fairness and capacity to effectively manage complexity, as well as the understanding and utilisation of informal leadership in the network.

(29) Organisational Culture

Ten sources refer to cultural issues in collaborative networked organisations. Bilal, Daclin, and Chapurlat examine diversity as a "crucial characteristic" of a system of systems (the "engineering twin" of a CNO) [16]. Others see differences in organisational cultures as a significant deterrent to effective collaboration [48]. Yet others argue that adequate culture, in their case study—through professional peer pressure, is more conducive to shaping ideas, motivating and energising the workforce, than is the strict compliance to rules and regulations [63]. In any case, CNO leaders are advised to promote mutual respect, spirit and ethic of collaboration, culture of openness and sharing ideas, and to invest in advancing cultural competence and mutual understanding [64] and "communicative culture" [65].

(30) Competences

Forty percent of the analysed sources address CNO competences and learning. That includes:

- understanding of and developing the CNO expertise potential, seeking to build the network mass and also multidisciplinary competences;
- building CNO competences by sharing knowledge and exchanging skills [42];
- developing individual and organisational capabilities for intuitive thinking, complex data analysis and communication [46].

The issue of network competences (along with the access to new markets) is of particular importance in the process of identification, assessment and selection of new partners [66], as well as retaining existing partners. The purpose is to develop and maintain the requisite collaborative capability [58].

Individual and organisational learning is another venue in which to develop the network competences. The academic literature addresses a number of learning issues, including the learning process, self-learning, agile learning, learning mechanisms for transformation, incremental learning, and the adoption of common best practices for organisational learning.

(31) Risk Management

The role of risk is referenced in 14 academic sources, covering respectively the need for:

- Identifying and quantifying existing or potential hazards, for example at the level of communication, management and sharing of knowledge [67];
- major concerns related to the use of shared assets and risks of intellectual property infringement [15];
- reducing uncertainty [68];

- risk mitigation [48]; and
- sharing risks among network partners [52].

(32) Evidenceence-based Decision-Making

The importance of data- and evidence-based decision-making is referenced in nine sources. The implementation of this core principle of quality management according to the international standards (including the ISO 9000 series) requires putting in place organisational processes for systematic data collection [69] and maintaining a repository of network assets [33], including data, information and knowledge.

(33) Competitiveness

Aspects of competitiveness are addressed in the highest number of the analysed academic sources—39 sources or nearly 70 percent. This can be expected, since value, generated benefits and—for the profit-oriented organisations—market share, return on investments, etc., are the lead drivers for establishing collaborative networked organisations in the first place.

This governance objective was not among those studied in the interviews and the analysis of existing networked organisations, with the assumption that a collaborative networked organisation coming out of the project consortium would have the technical capacity and organisational performance to be among the top most competitive suppliers of cybersecurity services; hence the focus there was on other governance issues.

The academic literature addresses, at times very comprehensively, aspects of competitiveness like:

- effectiveness;
- involving the most suitable partners with complementary competencies and providing access to new markets;
- customer-focus;
- reduced time to market;
- lower costs;
- delivery of services and products of higher quality;
- larger service and product portfolio;
- enhanced enterprise assets value;
- faster delivery;
- reliability;
- efficiency; etc.

Among the tools to achieve a differentiated competitive advantage, the academic literature suggests performance management, collaborative process management, business process alignment, effective and timely resource coordination, quality control, etc.

Figure 1 visualises the ranking of governance issues as they are referenced in the selected academic sources.

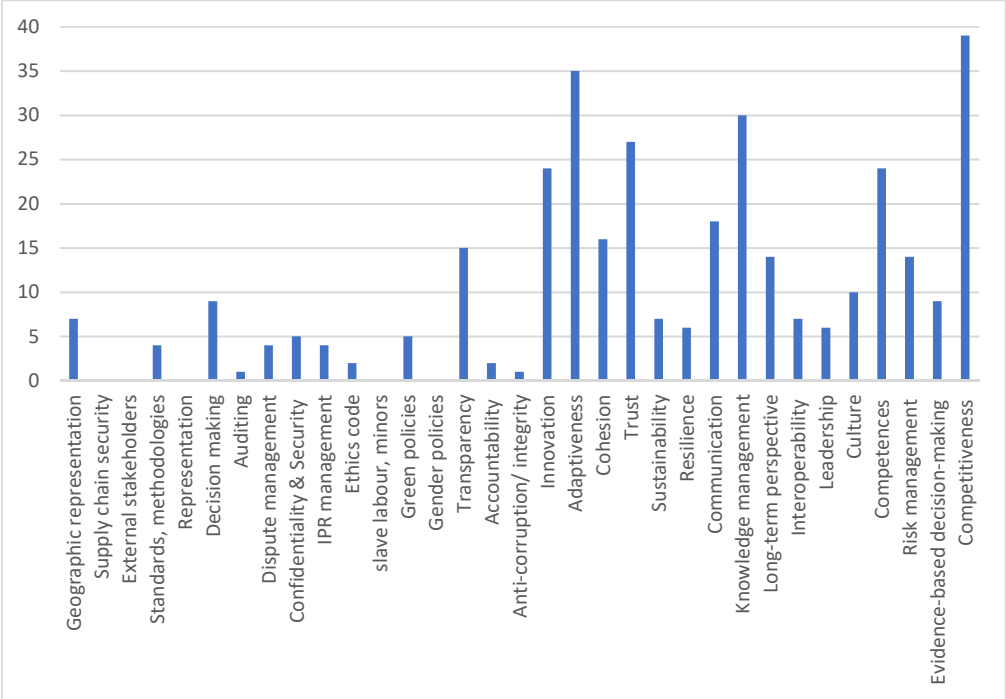

Figure 1. Number of referencing academic sources per governance issue.

3.3. Normative Requirements to Networks' Governance

The analysis of EU regulations and the main governance documents of the four pilot projects (14 documents in total) allowed to identify both explicitly stated and implicit requirements to the governance of networked organisations. Figure 2 presents the ranking for all 33 governance issues. According to current norms, of highest priority are the issues of geographic representation in the network organisation, implemented standards and methodologies, auditing, confidentiality and security, the network cohesion, trust, competences, risk management, and evidence-based decision-making.

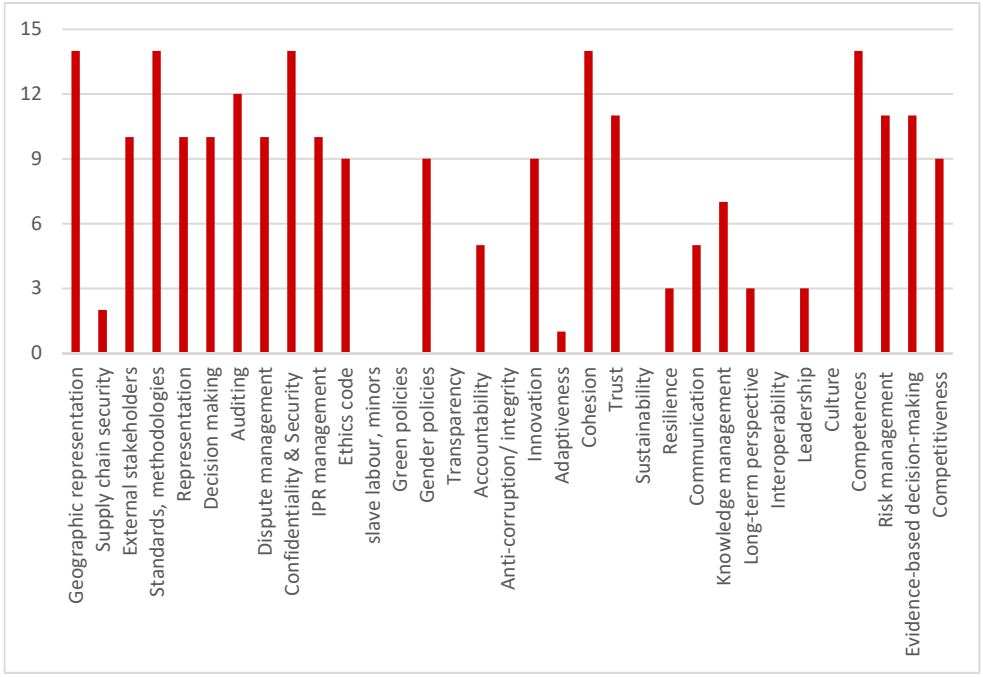

Figure 2. Number of normative documents referencing each governance issue.

3.4. Governance Issues in Statutory Documents of Existing Networks

The analysis of bylaws and other statutory documents of existing networked organisations provided numerous examples of the ways in which governance requirements are addressed in practice. Three governance categories appeared in the highest priority tier: representation of members on senior governance bodies of the network, knowledge management, and strategy-based long-term perspective on the collaboration. The full ranking is represented in Figure 3.

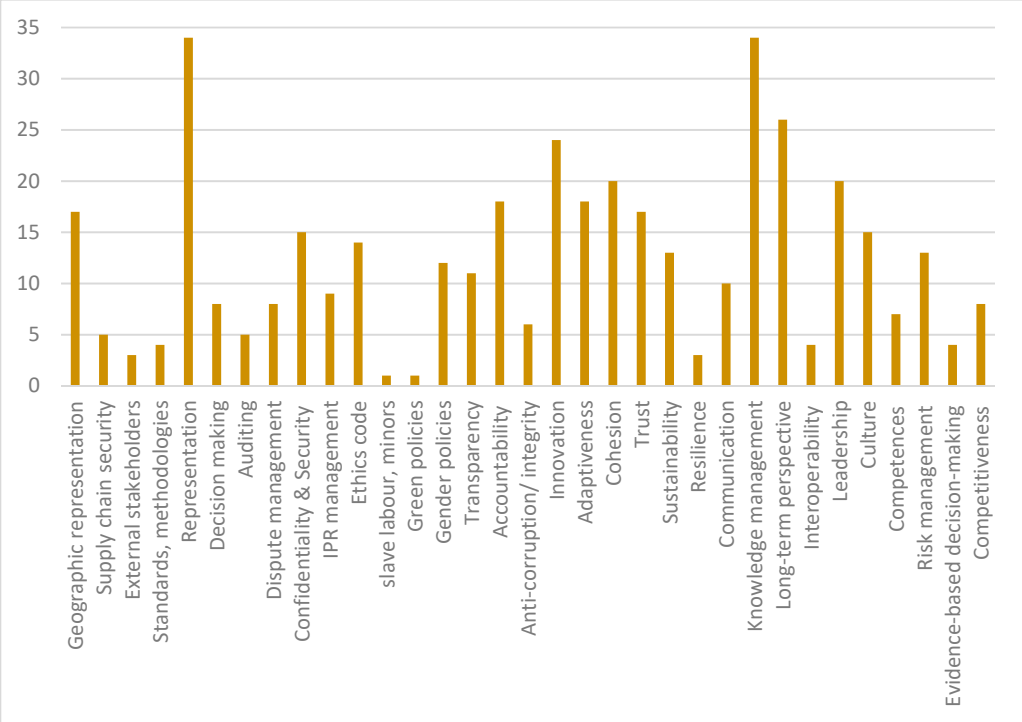

Figure 3. Number of existing networked organisations referencing each governance issue in their statutory documents.

3.5. Summary on Governance Objectives and Requirements

Table 2 presents the prioritised list of governance needs, objectives and requirements. It was constructed adhering to the following method.

First, all governance issues were split into 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 Table 2);
- 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 Table 2.

In the secondary analysis, all these governance issues were 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.).

In Table 2 each governance issue is placed in the highest tier it appears in the secondary analysis, i.e., even if it appears only once in Tier 1, e.g., *engaging external stakeholders* in the interviews, *adaptiveness* in the academic literature, and *trust* in norms and regulations, it is included in Tier 1 of the summary table below.

Table 2. Prioritisation of governance needs, objectives, and requirements.

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

4. Conclusions

The study of EU norms and regulations related to existing and prospective cybersecurity competence networks, statutory documents of networked organisations, academic sources and the opinion of interviewed stakeholders allowed to identify 33 categories of governance issues. Twenty-four of them are classified as "objectives" that can be pursued by devising and effectively implementing a consistent set of organisational measures, and another nine—as desired features of collaborative networked organisations that are context dependent and can be addressed directly only to an extent. Further, the governance categories were placed in four tiers, depending on the number of times a category has been referenced in primary sources. Placement of a governance issue in the highest tier (Tier 1) is indicative of the potentially highest priority of that issue.

The list of governance issues will be used to inform the development of alternative governance models and a weighted set of criteria for their evaluation by the research team in follow-on research. That will allow us to make an informed decision on the most appropriate governance model (or models) for the future cybersecurity network.

This prioritisation is expected to orient the development of alternative governance models and their evaluation, and not to predetermine the actions of the research team. It is possible that additional considerations may come into play in the meantime, e.g., requirements and expectations in the final version of Regulation 630.

To the author's knowledge, this is the first comprehensive study of the needs, objectives, and requirements to the governance of collaborative networked organisations in the field of cybersecurity. While it has been conducted with the specific needs of the Horizon 2020 call and the description of activities for a concrete project, the results may be of use to other endeavours towards arranging cybersecurity collaborative formats, as well as for the EU ambition to establish a European industrial, technology and research cybersecurity competence centre and a network of national coordination centres. They can be of use also in developing architectures, infrastructures and a broad variety of tools supporting collaboration in networked organisations.

Supplementary Materials: The following are available online at http://www.mdpi.com/1999-5903/12/4/62/s1, List of analysed network organisations, List of analysed academic sources.

Funding: 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.

Acknowledgments: The author gratefully acknowledges the contribution of Consuelo Colabuono from RHEA Group and Bríd Á. Davis from the National University of Ireland Maynooth who coded the references to governance issues respectively in directives and other norms and statutory documents of existing networked organisations.

Conflicts of Interest: The author declares no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

References

1. Goel, S. National Cyber Security Strategy and the Emergence of Strong Digital Borders. *Connect. Quart. J.* **2020**, 19. [CrossRef]
2. Spremić, M.; Šimunic, A. Cyber Security Challenges in Digital Economy. In Proceedings of the World Congress on Engineering WCE 2018, London, UK, 4–6 July 2018; pp. 341–346.
3. Singh, J.; Millard, C.; Reed, C.; Cobbe, J.; Crowcroft, J. Accountability in the IoT: Systems, Law, and Ways Forward. *Computer* **2018**, *51*, 54–65. [CrossRef]
4. Boeke, S. National cyber crisis management: Different European approaches. *Governance* **2018**, *31*, 449–464. [CrossRef]
5. Rondelez, R. Governing Cyber Security through Networks: An Analysis of Cyber Security Coordination in Belgium. *Int. J. Cyber Criminol.* **2018**, *12*, 300–315. [CrossRef]
6. Sharkov, G. From Cybersecurity to Collaborative Resiliency. In Proceedings of the 2016 ACM Workshop on Automated Decision Making for Active Cyber Defense SafeConfig, Vienna, Austria, 24 October 2016; pp. 3–9. [CrossRef]
7. Proposal for a Regulation of the European Parliament and of the Council establishing a European Cybersecurity Industrial, Technology and Research Competence Centre and a Network of National Coordination Centres (COM(2018) 630 Final). Available online: https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-cybersecurity-centres-regulation-630_en.pdf (accessed on 9 March 2020).
8. Establishing and Operating a Pilot for a Cybersecurity Competence Network to Develop and Implement a Common Cybersecurity Research & Innovation Roadmap. ID: SU-ICT-03-2018. 27 October 2017. Available online: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/su-ict-03-2018 (accessed on 9 March 2020).
9. Camarinha-Matos, L.M.; Afsarmanesh, H.; Galeano, N.; Molina, A. Collaborative Networked Organizations—Concepts and Practice in Manufacturing Enterprises. *Comput. Ind. Eng.* **2009**, *57*, 46–60. [CrossRef]
10. Ouyang, L.; Yuan, Y.; Wang, F.-Y. A Blockchain-based Framework for Collaborative Production in Distributed and Social Manufacturing. In Proceedings of the IEEE International Conference on Service Operations and Logistics, and Informatics 2019, SOLI 2019, Zhengzhou, China, 6–8 November 2019; pp. 76–81. [CrossRef]
11. Ziolkowski, R.; Miscione, G.; Schwabe, G. Consensus through Blockchains: Exploring Governance across Inter-organizational Settings. In Proceedings of the International Conference on Information Systems 2018, ICIS 2018, San Francisco, CA, USA, 13–16 December 2018.
12. Buchanan, W.; Thuemmler, C.; Spyra, G.; Smales, A.; Prajapati, B. Towards Trust and Governance in Integrated Health and Social Care Platforms. In *Health 4.0: How Virtualization and Big Data Are Revolutionizing Healthcare*; Thuemmler, C., Bai, C., Eds.; Springer: Cham, Switzerland, 2017; pp. 219–231. [CrossRef]
13. Kumar, B. The (In) Security of Smart Cities: Vulnerabilities, Risks, Mitigation and Prevention. *Int. J. Eng. Adv. Technol.* **2019**, *8*, 464–470. [CrossRef]
14. Radanliev, P.; De Roure, D.; Nurse, J.R.C.; Nicolescu, R.; Huth, M.; Cannady, S.; Montalvo, R.M. Integration of Cyber Security Frameworks, Models and Approaches for Building Design Principles for the Internet-of-Things in Industry 4.0. In Proceedings of the Living in the Internet of Things: Cybersecurity of the IoT, London, UK, 28–29 March 2018. CP740. [CrossRef]
15. Su, Z.; Biennier, F.; Ouedraogo, W.F. A Governance Framework for Mitigating Risks and Uncertainty in Collaborative Business Processes. In *Collaborative Networks in the Internet of Services*; Camarinha-Matos, L.M., Xu, L., Afsarmanesh, H., Eds.; Springer: Heidelberg, Germany, 2012; pp. 667–674.
16. Bilal, M.; Daclin, N.; Chapurlat, V. Collaborative Networked Organizations as System of Systems: A Model-Based Engineering Approach. In *Collaborative Systems for Smart Networked Environments, IFIP Advances in Information and Communication Technology*; Camarinha-Matos, L.M., Afsarmanesh, H., Eds.; Springer: Berlin/Heidelberg, Germany, 2014; Volume 434, pp. 227–234.
17. Dotsenko, S.; Illiashenko, O.; Kamenskyi, S.; Kharchenko, V. Integrated Security Management System for Enterprises in Industry 4.0. *Inf. Secur. Int. J.* **2019**, *43*, 294–304. [CrossRef]
18. Hütten, M. The Soft Spot of Hard Code: Blockchain Technology, Network Governance and Pitfalls of Technological Utopianism. *Glob. Netw.* **2019**, *19*, 329–348. [CrossRef]

19. Saleem, J.; Hammoudeh, M.; Raza, U.; Adebisi, B.; Ande, R. IoT Standardisation: Challenges, Perspectives and Solution. In Proceedings of the 2nd International Conference on Future Networks and Distributed Systems, Amman, Jordan, 26–27 June 2018. [CrossRef]
20. Eichensehr, K.E. Public-Private Cybersecurity. *Tex. Law Rev.* **2017**, *95*, 467–538.
21. Newlove-Eriksson, L.; Giacomello, G.; Eriksson, J. The Invisible Hand? Critical Information Infrastructures, Commercialisation and National Security. *Int. Spect.* **2018**, *53*, 124–140. [CrossRef]
22. Skierka, I.M. The Governance of Safety and Security Risks in Connected Healthcare. In Proceedings of the Living in the Internet of Things: Cybersecurity of the IoT, London, UK, 28–29 March 2018. CP740. [CrossRef]
23. Radanliev, P.; De Roure, D.C.; Nurse, J.R.C.; Montalvo, R.M.; Cannady, S.; Santos, O.; Maddox, L.T.; Burnap, P.; Maple, C. Future Developments in Standardisation of Cyber Risk in the Internet of Things (IoT). *SN Appl. Sci.* **2020**, *2*, 169. [CrossRef]
24. Leppänen, A.; Kankaanranta, T. Co-production of Cybersecurity: A Case of Reported Data System Break-ins. *Police Pract. Res. Int. J.* **2020**, *21*, 78–94. [CrossRef]
25. Deljoo, A.; Van Engers, T.; Koning, R.; Gommans, L.; De Laat, C. Towards Trustworthy Information Sharing by Creating Cyber Security Alliances. In Proceedings of the 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications and 12th IEEE International Conference on Big Data Science and Engineering, Trustcom/BigDataSE 2018, New York, NY, USA, 1–3 August 2018; pp. 1506–1510. [CrossRef]
26. Narendra, N.C.; Norta, A.; Mahunnah, M.; Ma, L.; Maggi, F.M. Sound Conflict Management and Resolution for Virtual-Enterprise Collaborations. *Serv. Oriented Comput. Appl.* **2016**, *10*, 233–251. [CrossRef]
27. Nurse, J.R.C.; Radanliev, P.; Creese, S.; De Roure, D. If You Can't Understand It, You Can't Properly Assess It! The Reality of Assessing Security Risks in Internet of Things Systems. In Proceedings of the Living in the Internet of Things: Cybersecurity of the IoT, London, UK, 28–29 March 2018. [CrossRef]
28. Wulf, A.; Butel, L. Knowledge Sharing and Collaborative Relationships in Business Ecosystems and Networks: A Definition and a Demarcation. *Ind. Manag. Data Syst.* **2017**, *117*, 1407–1425. [CrossRef]
29. Rantos, K.; Spyros, A.; Papanikolaou, A.; Kritsas, A.; Ilioudis, C.A.; Katos, A. Interoperability Challenges in the Cybersecurity Information Sharing Ecosystem. *Computers* **2020**, *9*, 18. [CrossRef]
30. Scala, N.M.; Reilly, A.C.; Goethals, P.L.; Cukier, M. Risk and the Five Hard Problems of Cybersecurity. *Risk Anal.* **2019**, *39*, 2119–2126. [CrossRef]
31. European Network of Cybersecurity Centres and Competence Hub for Innovation and Operations (ECHO). Available online: https://echonetwork.eu/ (accessed on 10 March 2020).
32. Kalkman, J.P.; Wieskamp, L. Cyber Intelligence Networks: A Typology. *Int. J. Intell. Secur. Public Aff.* **2019**, *21*, 4–24. [CrossRef]
33. Tapia, R.S. Converging on Business-IT Alignment Best Practices: Lessons Learned from a Dutch Cross-Governmental Partnership. In Proceedings of the 2009 IEEE International Technology Management Conference (ICE), Leiden, The Netherlands, 22–24 June 2009. [CrossRef]
34. Rabelo, R.J.; Costa, S.N.; Romero, D. A Governance Reference Model for Virtual Enterprises. In *Collaborative Systems for Smart Networked Environments, IFIP Advances in Information and Communication Technology*; Luis, M., Camarinha-Matos, L.M., Afsarmanesh, H., Eds.; Springer: Berlin/Heidelberg, Germany, 2014; Volume 434, pp. 60–70.
35. Slayton, R. Governing Uncertainty or Uncertain Governance? Information Security and the Challenge of Cutting Ties. *Sci. Technol. Hum. Values* **2020**. [CrossRef]
36. Pohle, J. Multistakeholder Governance Processes as Production Sites: Enhanced Cooperation in the Making. *Internet Policy Rev.* **2016**, 5. [CrossRef]
37. Feenberg, A. The Internet as Network, World, Co-construction, and Mode of Governance. *Inf. Soc.* **2019**, *35*, 229–243. [CrossRef]
38. Sterlini, P.; Massacci, F.; Kadenko, N.; Fiebig, T.; Van Eeten, M. Governance Challenges for European Cybersecurity Policies: Stakeholder Views. *IEEE Secur. Priv.* **2020**, *18*, 46–54. [CrossRef]
39. Kvale, S.; Brinkmann, S. *InterViews: Learning the Craft of Qualitative Research Interviewing*, 2nd ed.; SAGE: Los Angeles, CA, USA, 2009.
40. Brymann, A. *Social Research Methods*, 4th ed.; Oxford University Press: Oxford, UK, 2012.

41. Tagarev, T. Governance of Collaborative Networked Organisations: Stakeholder Requirements. In Proceedings of the 11th IEEE International Conference on Dependable Systems, Services and Technologies DESSERT 2020, Kyiv, Ukraine, 14–18 May 2020.
42. Mortati, M. *Systemic Aspects of Innovation and Design: The Perspective of Collaborative Networks*; Springer: Cham, Switzerland, 2013.
43. Grippa, F.; Leitão, J.; Gluesing, J.; Riopelle, K.; Gloor, P. *Collaborative Innovation Networks: Building Adaptive and Resilient Organizations*; Springer: Cham, Switzerland, 2018. [CrossRef]
44. Kandjani, H.; Bernus, P. Towards a Cybernetic Theory and Reference Model of Self-designing Complex Collaborative Networks. In *Collaborative Net-Works in the Internet of Services*; Camarinha-Matos, L.M., Xu, L., Afsarmanesh, H., Eds.; Springer: Berlin/Heidelberg, Germany, 2012; pp. 485–493.
45. Hovorka, D.S.; Larsen, K.R. Enabling Agile Adoption Practices through Network Organizations. *Eur. J. Inf. Syst.* **2006**, *15*, 159–168. [CrossRef]
46. Crawford, K.; Hasan, H.M.; Warne, L.; Linger, H. From Traditional Knowledge Management in Hierarchical Organizations to a Network Centric Paradigm for a Changing World. *Emerg. Complex. Organ.* **2009**, *11*, 1–8.
47. Jackson, P.; Cardoni, A. Organizational Design and Collaborative Networked Organizations in a Data-Rich World: A Cybernetics Perspective. In *Collaboration in a Data-Rich World, IFIP Advances in Information and Communication Technology*; Camarinha-Matos, L.M., Afsarmanesh, H., Fornasiero, R., Eds.; Springer: Cham, Switzerland, 2017; Volume 506, pp. 185–193. [CrossRef]
48. Durugbo, C. Collaborative Networks: A Systematic Review and Multi-level Framework. *Int. J. Prod. Res.* **2016**, *54*, 3749–3776. [CrossRef]
49. Noran, O. Towards a Meta-Methodology for Collaborative Networked Organisations. In *Virtual Enterprises and Collaborative Networks, IFIP International Federation for Information Processing*; Camarinha-Matos, L.M., Ed.; Springer: Boston, MA, USA, 2004; Volume 149, pp. 71–78.
50. Jung, K. Sources of Organizational Resilience for Sustainable Communities: An Institutional Collective Action Perspective. *Sustainability* **2017**, *9*, 1141. [CrossRef]
51. Krčo SVan Kranenburg, R.; Lončar, M.; Ziouvelou, X.; McGroarty, F. Digitization of Value Chains and Ecosystems. In *Digital Business Models: Driving Transformation and Innovation*; Aagaard, A., Ed.; Palgrave MacMillan: Cham, Switzerland, 2019; pp. 81–116. [CrossRef]
52. Romero, D.; Molina, A. Collaborative Networked Organisations and Customer Communities: Value Co-Creation and Co-Innovation in the Networking Era. *J. Prod. Plan. Control* **2011**, *22*, 447–472. [CrossRef]
53. Barchetti, U.; Capodieci, A.; Guido, A.L.; Mainetti, L. Collaborative Process Management for the Networked Enterprise: A Case Study. In Proceedings of the 26th IEEE International Conference on Advanced Information Networking and Applications Workshops, Fukuoka, Japan, 26–29 March 2012; pp. 1343–1348. [CrossRef]
54. Hovorka, D.S.; Larsen, K.R. Increasing Absorptive Capacity through Strategic use of Network Organizations. In Proceedings of the 11th Americas Conference on Information Systems AMCIS 2005, Omaha, NE, USA, 11–14 August 2005; p. 270.
55. Rostek, K. *Benchmarking Collaborative Networks: A Key to SME Competitiveness*; Springer: Cham, Switzerland, 2015.
56. Pawlak, A.; Jørgensen, H.D. Holistic Design of Collaborative Net-works of Design Engineering Organizations. In *Risks and Resilience of Collaborative Networks, IFIP Advances in Information and Communication Technology*; Camarinha-Matos, L.M., Bénaben, F., Picard, W., Eds.; Springer: Cham, Switzerland, 2015; Volume 463, pp. 612–621.
57. Serrier, S.B.; Ducq, Y.; Vallespir, B. Networked Companies and a Typology of Collaborations. In *Enterprise Interoperability: INTEROP-PGSO Vision*; Archimède, B., Vallespir, B., Eds.; Wiley-ISTE: London, UK, 2017; Volume 1, pp. 19–42. [CrossRef]
58. Ulbrich, S.; Troitzsch, H.; Van den Anker, F.; Plüss, A.; Huber, C. How Teams in Networked Organisations Develop Collaborative Capability: Processes, Critical Incidents and Success Factors. *Prod. Plan. Control Manag. Oper.* **2011**, *22*, 488–500. [CrossRef]
59. Cardoni, A.; Saetta, S.; Tiacci, L. Evaluating How Potential Pool of Partners Can Join Together in Different Types of Long Term Collaborative Networked Organizations. In *Collaborative Networks for a Sustainable World, IFIP Advances in Information and Communication Technology*; Camarinha-Matos, L.M., Boucher, X., Afsarmanesh, H., Eds.; Springer: Berlin/Heidelberg, Germany, 2010; Volume 336, pp. 312–321.

60. Saetta, S.; Tiacci, L.; Cagnazzo, L. The Innovative Model of the Virtual Development Office for Collaborative Networked Enterprises: The GPT Network Case Study. *Int. J. Comput. Integr. Manuf.* **2013**, *26*, 41–54. [CrossRef]
61. Andres, B.; Poler, B.; Sanchis, R. Collaborative Strategies Alignment to Enhance the Collaborative Network Agility and Resilience. In *Risks and Resilience of Collaborative Networks, IFIP Advances in Information and Communication Technology*; Camarinha-Matos, L.M., Bénaben, F., Picard, W., Eds.; Springer: Cham, Switzerland, 2015; Volume 463, pp. 88–99.
62. Durugbo, C.; Riedel, L.C.K.H. Readiness Assessment of Collaborative Networked Organisations for Integrated Product and Service Delivery. *Int. J. Prod. Res.* **2013**, *51*, 598–613. [CrossRef]
63. Mabey, C.; Wong, A.L.Y.; Hsieh, L. Knowledge Exchange in Networked Organizations: Does Place Matter? *R D Manag.* **2014**, *45*, 487–500. [CrossRef]
64. Song, Y.; Grippa, F.; Gloor, P.A.; Leitão, J. (Eds.) *Collaborative Innovation Networks: Latest Insights from Social Innovation, Education, and Emerging Technologies Research*; Springer: Cham, Switzerland, 2019.
65. Enquist, H.; Nilsson, A.; Magnusson, J. Change Management Implications for Network Organizations. In Proceedings of the 37th Annual Hawaii International Conference on System Sciences, Big Island, HI, USA, 5–8 January 2004. [CrossRef]
66. Arrais-Castro, A.; Varela, M.L.R.; Putnik, G.D.; Ribeiro, R.A.; Machado, J.; Ferreira, L. Collaborative Framework for Virtual Organization Synthesis Based on a Dynamic Multi-criteria Decision Model. *Int. J. Comput. Integr. Manuf.* **2018**, *31*, 857–868. [CrossRef]
67. Abreu, A.; Calado, J.M.F. Risk Model to Support the Governance of Collaborative Ecosystems. *IFAC PapersOnLine* **2017**, *50*, 10544–10549. [CrossRef]
68. Komanda, M. Foundations of Network Organizations Ontology. *Int. J. Bus. Manag. Stud.* **2012**, *1*, 565–569.
69. Pierce, P.; Ricciardi, F.; Zardini, A. Smart Cities as Organizational Fields: A Framework for Mapping Sustainability-Enabling Configurations. *Sustainability* **2017**, *9*, 1506. [CrossRef]