Information & Security

A. Pasic
vol. 53, no. 1 (2022): 105-130
https://doi.org/10.11610/isij.5308

Published since 1998

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

Research Article

Governance Mesh Approach for Cybersecurity Ecosystem

Aljosa Pasic (✉)

Atos Spain, Madrid, Spain, https://atos.net/

ABSTRACT:

Four EU pilot projects have been launched in 2019 (ECHO, SPARTA, CSEU, and CONCORDIA) with the focus on specific context of EU Regulation that is establishing the European Cybersecurity Competence Centre (ECCC), together with the Network of National Coordination Centers (NCCs), and Competence community (CC). These projects are continuously providing their feedback on open issues regarding the overall governance in this emerging EU cybersecurity ecosystem. We look at similar cybersecurity initiatives from the past, as well as related work. While hybrid governance model, that combines top-down and bottom-up elements seems to be the most reasonable and acceptable outcome for all communities involved, there is a further need to decompose complex model and perform precise analysis of Processes, Rules, Norms, and Actions (PRNA), linked to fundamental areas of work of this ecosystem (e.g., capacity building, incident response, R&D management etc.). This article provides an overview of several challenges that need to be addressed and presents the approach to governance we call "governance mesh."

ARTICLE INFO:

RECEIVED: 28 JUNE 2022
REVISED: 17 AUG 2022
ONLINE: 21 SEP 2021

KEYWORDS:

cybersecurity governance; cybersecurity ecosystems; cybersecurity mesh

✉ Corresponding Author: E-mail: aljosa.pasic@atos.net

Introduction

The European Union has articulated its ambition to the area of cybersecurity in several ways, for example, through the EU's Cybersecurity Strategy for the Digital Decade.[1] Recent Regulation (EU) 2021/887 of the European Parliament and of the Council (in further text "ECCC regulation") is, in this direction, a key document that also lists main challenges in the area of cybersecurity. Examples of these challenges are the lack of cooperation between Member States, industries and academia, fragmented efforts in research and development (R&D), insufficient investment, increased demand for cybersecurity skills, or inconsistency in policies, legal frameworks and actual practice. It is also addressing establishment of the European Cybersecurity Competence Centre (ECCC), together with the Network of National Coordination Centres (NCCs), and Competence community (CC).[2]

We take this document as the starting point, context for which we make several key definitions of concepts or terms used in governance model. It is also a starting point for the four EU pilot projects launched in 2019, when draft of ECCC regulation [3] was still leaving many uncertainties. These four pilot projects (ECHO, SPARTA, CSEU and CONCORDIA),[4] that are piloting cybersecurity competence community (CC), are also expected to continuously provide their feedback on open issues regarding the overall governance and relations between ECCC, located in Bucharest, network of member state located NCCs, and CC. In addition, several inter-pilot collaboration meetings with focus on governance, have been done with the aim of convergence of different approaches around so called "umbrella alternative." This paper is giving an overview of different approaches and opinions expressed in four projects, having in mind that this consultation is still an open process, while it is also introducing a new concept of "governance mesh" model that would take the best of each four pilot projects, enhanced with the other external contributions. Unlike an overarching "umbrella approach," it would promote co-existence and interoperability of different "governance models" in an attempt to bring together all different hubs, communities, networks and other forms of collaboration in cybersecurity.

In addition, we look back and present lessons learned from the previous EU cybersecurity community-building initiatives, as well as an overview of the related work from the other domains. In some cases, we highlight if there are any aspects that could also be applicable to the cybersecurity context. In a similar way, we also give a brief overview of theoretical work on network structures, value co-creation, and the evolution of related concepts such as communities, constellations, or ecosystems.

This leads us to an analysis of a hybrid governance model that addresses gaps that have been found not only in the four pilot projects but also in many other R&D cybersecurity projects. From well-known challenges related to the shortage of skills to persisting issues such as stakeholder incentives, we advocate for breaking-up complex and overarching governance models, into a topic or function specific analysis of Processes, Rules, Norms, and Actions (PRNA), that would

help to address three governance model pillars (who, what and how) in a piecemeal manner. In some cases, top-down, in others bottom-up, sometimes technology push, another research pull: we finish this "governance mesh" approach with a set of conclusions and recommendations that should be crystalized in the final stage of work of four pilot projects, and that should contain enough flexibility to adapt to dynamic and complex environment, such it is cybersecurity in EU.

Methods

Methodology and procedure applied for the development of the article is largely based on methodology for validation of the governance structure in Cybersecurity4Europe and explained in detail in deliverable D2.2 Internal Validation of Governance Structure.[11] It includes comprehensive understanding of the issues related to governance structure validation but is additionally enhanced with lessons learned from the previous cybersecurity ecosystem building approaches, documented in relevant reports, as well as the subjective opinions from author that participated in these ecosystems. These issues are grouped into three categories:

- Structure (e.g., lifecycle and procedures for the "substructures" such as working groups)
- Stakeholders and rules (e.g., participation or decision-making rules)
- Objectives, support services, and areas of engagement (e.g., transfer of technology, pooling of R&D resources)

For this last category of issues, inputs that have been received from stakeholders in Cybersecurity4Europe, have been further filtered, mapped into "strategic areas," and contrasted with external information, such as member state ecosystem development status, relevant EC policy and legislative drafting, or ongoing work in the other pilots. After inter-pilot governance collaboration proposed an "umbrella alternative," a term and a hypothesis on cybersecurity governance "mesh" started to be developed. The next step in the methodology, outside of the scope of this paper, would be more specific and detailed shaping of identified clusters and strategic areas into governance "mesh" concept, with focus on specific processes, rules, norms, and actions.

Context

Word "network" is mentioned 53 times in ECCC regulation (plus few mentions of related terms). Word "community" is mentioned 70 times, while the word "ecosystem" is mentioned only twice. In Article 4, for example, it is mentioned that "Objectives of the Competence Centre should be contributing to a strong European cybersecurity ecosystem which brings together all relevant stakeholders."

Yet, in discussion among stakeholders in pilot projects of CC, as well as among other participants from different projects, the word "ecosystem" seems to be

preferred term, when addressing the new multi-level, multi-stakeholder structure created by the ECCC regulation. Different words could mean different things for different people, so we start with definitions that will be used throughout this document. If there is no explicit reference, definitions are based on those from online Oxford dictionary.[5]

Word "net" and its extension "network" could, in our context, refer to both the subject and the object of governance model. Dictionary defines it as "a closely connected group of people, companies, etc. that exchange information," but also as "a number of computers and other devices that are connected together so that equipment and information can be shared." Definition of network security could be also found in ISO/IEC 27033-1:2015 that provides an overview of network security and related terms. Another semantic twist was added with prefix "inter," when existing nets (Hepnet, Telenet, Span, Arpanet…) became interconnected thanks to TCP/IP, one of the first open interoperability protocols. More importantly for our context, early internet was designed without security in mind, a decision that had consequences until today.

Cybersecurity, or security in cyberspace is, however, not the same as security of the internet, in the same way that internet, web and cyberspace are not exactly synonyms. Standard ISO/IEC 27032:2012 [7] provides guidance on what is called "the unique aspects" of cybersecurity in respect to information security, network security, internet security, and critical information infrastructure protection (CIIP). Whether these aspects, defined as the protection of privacy, integrity, availability, and confidentiality of information in the Cyberspace, are unique, is questionable, since they also appear in many other standards and definitions, for example ISO/IEC 27000:2018 overview of information security management systems (ISMS). As for the "ecosystem" and stakeholder communities, the most of "cybersecurity community" was involving same stakeholders as "information security community," "CIIP community" and others, where author of this article was personally participating.

This brings us to term "community." While network is characterized by nodes, relationships and topology, community is characterized by rather vaguely, being often reduced to "stakeholder group that has something in common." We should consider and acknowledge co-existence of different cybersecurity communities and different categorization of those communities (e.g., research, industry, cryptography, assurance and certification, national, regional etc). Here, the important effort was done by Joint Research Centre (JRC), the European Commission's science and knowledge service, that created taxonomy of cybersecurity research domains, sectorial dimensions, as well as the application and technology dimensions.[8] By applying it, one could talk about research community in domain of cryptology, industry community in the sector of defence or, for example, start-up community in Internet of Things (IoT) cybersecurity.

Existence of so many communities and sub-communities, with various degrees of overlapping and interconnections, as well as the existence of related

resources (e.g., testbeds, datasets), practices (e.g., awareness building, certification of skills) or technologies, is bringing us to the definition of "ecosystem."

CONCORDIA deliverable defines ecosystem as "a system of people, practices, values, and technologies in a particular environment,"[9] that, according to ECHO project deliverable, includes "roles, tasks, and relationships, which could be customized for different layers or even different member states." [10] Unlike the concept of a network, ecosystem also brings several layers and links with the other disciplines (legal, economic etc.) since different issues need to be considered from multiple perspectives. An "ecosystem" is therefore a socio-technical construction where objectives such as reuse of shared resources or scale-up of new solutions, need to be achieved by synergy between (sub)communities, but also by trade-offs and consensus.

SPARTA deliverable [12] considers taking up "relevant active digital ecosystems and public-private cooperation models," while this project claims to "build on recognized national ecosystems (France, Italy, and Lithuania) and complementary formal, applied and social disciplines." The fourth pilot project for the CC is Cybersecurity4Europe, and it is using word "ecosystem" more cautiously, although states that "ECSO is a comprehensive representation of the full cybersecurity ecosystem." [11] Indeed, the European Cyber Security Organisation (ECSO) claims, on its web page, that the main goal of ECSO is to coordinate the development of the European Cybersecurity Ecosystem.[13]

Lessons Learned from past EU initiatives in Cybersecurity

The European Cyber Security Organisation (ECSO) ASBL is a non-for-profit organisation under the Belgian law, established in June 2016. At that time, it was the contractual counterpart to the European Commission for the implementation of the Cyber Security contractual Public-Private Partnership (cPPP) with the European Commission. Governance model for this cPPP was rather simple,[14] with partnership board, members and ECSO acting as a secretariat. Although ECSO members include a wide variety of stakeholders, either involved directly or represented through their community managers, it was supposed to be industry driven organization. Its roots lie in the European Organisation for Security (EOS),[15] which, in its turn, was established as a kind of "spin-off" from Aerospace and Defence Industry Association (ASD).[16]

Industry focus of ECSO is also marked by the launch, on June 7th, of the Chief Information Security Officers (CISOs) European Community (CEC). In this community, membership is open and is free to ECSO members' CISOs, but also to non-ECSO members CISOs.[17] Whether other communities or sub-communities will emerge from ECSO, is not clear at this stage. Some initiatives, such as the European Cybersecurity Investment Platform (ECIP), European Cybersecurity STARtup Award and Cyber Investor Days, have been particularly relevant for start-ups and cybersecurity investment community, and might be consolidated into a more stable or formal structure.

ECSO is, by no means, the first example of "cybersecurity ecosystem" in Europe. There have been different attempts in the past, albeit short-lived, and we can learn some lessons from them.

The EP3R (European Public-Private Partnership for Resilience) was established in 2009 and closed in April 2013. In ENISA report [18] it was described as "the very first attempt at Pan-European level to use a Public-Private Partnership (PPP) to address cross-border Security and Resilience concerns in the Telecom Sector." This statement might be questionable since it was not a contractual PPP. In addition, different communities with information security focus have been already existing in several European initiatives,[19, 20] organized as the working groups of larger initiatives (such as European technology Platforms) and co-funded by the European Commission within the Sixth Framework Programme (2002-2006).

The EP3R, however, had an important support from European Union Agency for Cybersecurity (ENISA), that initiated, supported, and participated in many discussions. The PPP approach was judged to be particularly appropriate for addressing complex cooperation problems and the model was even proposed for Information Sharing and Analysis Centres (ISACs) and similar structures. Initially, the EP3R was facing challenges and value propositions such as team building, trust, joint objectives, and action plan identification, all of them relevant until today. Many of the initial stakeholders lost interest, soon after its launch. In a survey about the work of EP3R, stakeholders mentioned a couple of shortcomings and recommendations, such as the need for smaller working groups, focused and limited in time, need to improve motivation and incentives of demand side stakeholders, simple but formal rules of governance and others. In 2011 ENISA published a Good Practice Guide on Cooperative Models for Effective PPPs [21] and included some of these opinions in this report.

Private-Public Partnerships (PPP) were already a well-known instrument that has been used many times since the Commission published Guidelines for Successful Public–Private Partnerships [22] in 2003. However, after some criticism about too many "self-proclaimed PPPs," the Commission added word "contractual" to cPPP, to distinguish these as more formal forms of PPP with the EC. ENISA made distinction between institutional PPP, goal-oriented PPP, outsourcing PPP and hybrid PPP.[21] It also gave brief comment on governance models of each of these types.

Maybe, for this reason, the establishment of the Network and Information Security (NIS) PPP was announced as the "Public-Private Platform" instead of "partnership" in the EC communication about the Cybersecurity Strategy of the European Union in 2013.[23] The same document is also mentioning "public-private partnerships" like EP3R (dysfunctional at that moment) and Trust in Digital Life (TDL),[24] one of these initiatives that was initially marketed as PPP, later changed into "membership association" (TDL is also partner in Cybersecurity4Europe project).

The NIS Platform was supposed to complement and underpin the proposed NIS Directive, while at the same time its subsections (working groups) were addressing more specific objectives, such as the research road mapping, or assessment of Business Cases and Innovation Paths. The Commission has called the first plenary meeting of the NIS platform on 17 June 2013, but this initiative, like EP3R, was short-lived. Nevertheless, NIS Platform served to pave the way for the European Cyber Security Organization (ECSO), as many of the initial stakeholders were the same. It can be seen as an important step in the consolidation and convergence of different communities, as well as the ecosystem building step.

Finally, we should also mention the previous EU cybersecurity initiatives that would qualify as "communities" but maybe not as the full cybersecurity "ecosystems." These often have very focused objectives, such as data sharing. ENISA conducted a study on Cooperative Models for Public-Private Partnership (PPP) and Information Sharing and Analysis Centres (ISACs),[25] collating information on best practices and common approaches. In cybersecurity research, on the other hand, there are many useful initiatives and lessons learned, for example from EU 7th framework programme, where "Network of Excellence" (NoE) were designed for research institutions willing to combine and functionally integrate part of their activities and capacities in a given field. These NoE were creating de facto "virtual research centres" in specific cybersecurity areas, such as secure software and services in NESSOS project,[26] or European Network of Excellence in Cryptology ECRYPT 2.[27]

Table 1. An overview of governance approaches and issues in the past EU cybersecurity initiatives.

Initiative	Structure	Stakeholders and rules	Areas and services
ECSO	Board of Directors with several fixed committees and more flexible working groups. Task-forces (e.g., cloud security) and transversal initiatives (e.g., Woman4Cyber) are also contemplated.	Structure and rules are aligned with different categories of stakeholders (e.g., national authorities, industry, SMEs etc.)	Wide coverage of topics, from policy inputs to labels "cybersecurity made in EU"
EP3R	Originally structured on three Working Groups (WG). Structural changes after mid-2012 with	Only invited experts from National and pan European Telecom operators, Internet	Information sharing and stock taking of good policy and industrial practices (methodology to classify assets

	moderators. Initial areas gradually evolved into smaller sub-groups, replaced by Task Forces.	Service Providers, industrial associations, Standardisation Bodies, Competent National Authorities, manufacturers, and solution providers	supporting CIIs infrastructures, reliability, resilience, and security levels of equipment etc.). Later also policy discussion and recommendations (e.g., to implement a pan-European botnet-fighting programme)
NIS Platform	The launch meeting in June 2013, established 3 working groups, each one with two chairs, one from the public and one from private sector.	WG3 proposed the set of categories that captured the distinct perspectives e.g. from demand perspective (end user, regulator, owner/operator, dependent third party), from innovation perspective, from sector and size perspective (defense and intelligence, enterprises, SMEs, consumers) etc.	Identify the possible scenarios for cybersecurity in the medium/long term risk management, including information assurance, risks metrics and awareness raising, information exchange and incident coordination
"Network of Excellence" (NoE) NESSOS	Different boards and Networking and Liaison Advisory Board (NaLAB), Network Activity Board (NAB), Industry Advisory Group etc	Mainly research stakeholders in secure software engineering	Re-address, integrate, harmonize, and foster the research activities, spread the research excellence, collaborate with industrial stakeholders to improve the industry best practices

Approach to Governance from Four CC Pilot Projects

The pilot projects of cybersecurity competence community (ECHO, SPARTA, CSEU and CONCORDIA)[28] are the four winning projects of the 2018 Horizon

2020 cybersecurity call related to "establishing and operating a pilot for a European Cybersecurity Competence Network and developing a common European Cybersecurity Research and Innovation Roadmap." Many partners of these four projects have also been present in the initiatives described in the previous chapter and can be considered as representative stakeholders of EU cybersecurity communities. Together, four projects bring more than 160 partners, with overall EU investment of more than 63.5 million Euros.

The four projects made several proposals related to the governance model of the forthcoming ecosystem, and in particular for the cybersecurity community (CC) part of it. Cybersecurity4Europe project, that has work package dedicated to governance modelling, is proposing a network of Community Hubs of Expertise in Cybersecurity Knowledge (CHECKs),[29] as a kind of the bottom-up approach to integrate sub-structures of the cybersecurity community with the rest of ecosystem. There have been several categories of CHECKs under consideration, as well as several processes, rules, norms an action (PRNA), including collective decision making, or coordination mechanism with external bodies. The model and its assumptions were validated in the real-life scenario, namely with cybersecurity stakeholders in Toulouse in an entity named CHECK-T (CHECK toulouse).[11]

There is an inevitable comparison of CHECKs to Digital Innovation Hubs (DIHs), a kind of structure that exists with this name from 2016. Originally, DIHs were linked to the Digitizing European Industry (DEI) initiative.[30] Afterwards, the DIH concept was also evolving towards the European DIH (E-DIH) and outside of Industry sector. More recently, it has also been suggested to use DIH as a model for regional or national cybersecurity community structures.

There was an attempt [31] to establish a shared common conceptual framework of a DIH within the European DIH stakeholders. This included five different building blocks as the backbone of the European DIH network, roughly described around competences, services, economy, finance and, finally, collaborations and networks. One of the distinctive features of "DIH-based structure" is also focus on SMEs and Mid-caps, maybe due to the synergy established with a mechanism called "Smart Specialization Platform," where DIH were started to be used as a policy instrument to boost specific priorities.[32]

Elevated economic risks and market failures are common in cybersecurity, while "economies of scale," one of the main DIH assumptions, are also very important for cybersecurity ecosystem. Therefore, it does make sense to consider these structures, whether DIHs or CHECKs, as a part of CC governance model. The main problem remains, however, how would these interact with each other across member state borders, and what would be the role of NCC in establishing these cross-border links? Could multi-national organization be part of multiple DIH/CHECKs in different countries? Can there be European DIH/CHECK or can this organisation participate directly in the CC, without need to be part of national or regional hub?

ECHO project took several steps in designing the optimal Governance model for the CC and described it in deliverables,[33] including its main direction towards

the development of the future ECHO Collaborative Networked Organisation (CNO). The project used the Analytic Hierarchy Process (AHP) method to reach consensus among stakeholders, engaging European Cyber Security Organisation (ECSO) as well. The assessment of alternatives was done by comparison of governance model performance against several pre-defined criterions. The solution accepted by the most stakeholders was to create one "umbrella" alternative, so called Alternative 0 (A0), which could be based on best practices from the other four alternative models. ECHO was also the only pilot project that did the process landscape description and initial process discovery, by using COBIT (Control Objectives for Information and Related Technologies) as a framework.[34] Organizational structure design for the National Hubs (ECHO Chapters) is following the same model, while the ECHO Service Groups (SGs or Virtual Organisations – Vos) are supposed to be an equivalent to the CC. There are no details about the requirements to the Partners onboarding SG, although candidates should provide evidence that they have required experience, capacity, and capabilities for delivery of service. From the past experiences, we know that this is of–en a very delicate issue: exclude some stakeholders and SG(VO) could be accused of forming an "exclusive club"; leave it more open and it will risk having endless debates about every little detail. It is classical challenge in EU initiatives, but also well documented challenge in open-source communities, that describes struggle between top-down and bottom-up design.[35]

SPARTA project deals with governance in a more "lightweight" manner, describing the structures, processes and activities that characterize the governance of the SPARTA project itself,[36] and then moves into adequacy of this model for the CC in the context of ecosystem created under ECCC regulation. Conclusion was that there was strong utilization of some project committees and processes (e.g., road mapping), while the other governance model structures (notably the Certification Task Force, the Ethics Board, and the Advisory committee) were under-utilized in the project. SPARTA also envisages several "instruments," such as roadmap, partnership, or program. In this pilot project, four "programs" have been defined beforehand, with focus on: artificial intelligence (SAFAIR), high level assurance (HAII-T), continuous assessment (CAPE) and Cybersecurity Threat Intelligence Framework (T-SHARK). Activities within each Program have been divided into two main streams: one dedicated to technology-based developments (Sub-cases), and another for the supporting activities, including legal, exploitation, but also program governance support. Program governance activities are coordinated by L3CE (Lithuanian Cyber Crime Center of Excellence for Training, Research and Education).[37]

Finally, in the case of CONCORDIA pilot project, there are no specific activities or reports related to assessment of governance models in the context of the future ecosystem or the CC. However, there are already some services, offered for free, to specific cybersecurity communities, such as the catalogue of online training offerings and certification support for the cybersecurity capacity building, or informative services for start-up community.[38] There are also several

Table 2. Approaches and examples of governance issues discussed in four "ECCC regulation pilot projects."

Pilot project	Structure	Stakeholders and rules	Areas and services
CS4EU	Focus is on external validation (outside pilot project) of Community Hubs of Expertise in Cybersecurity Knowledge (CHECKs).[11] Issues discussed include: degree of the formalization of the lower-level structures; alignment to stakeholders' demands; the synergy between formal and informal, top-down and bottom-up structures; the flexibility of the structure, including the mechanisms to distribute the positions, delegate powers, and create additional structures; a possibility for the collaboration/merge between the two structures; the focus on regional versus EU interests; possible (sub)network of CHECKs.	List of stakeholders that participated in validation of CHECK model [11] with open issues such as: uncertainty over membership; way to motivate practitioners; mechanisms for participation of other disciplines; financing mechanisms; procedure for identification of "regional interests"; rules for a "bottom-up decision making."	Examples include: Research/ innovation; strategic decision making; alignment with local/ regional roadmaps; training and capacity building; mentoring aspects and seed capital investment strategies; space for experimentation
ECHO	Initial design has four key processes and three organizational structures: central hub (ECHO Collaborative Networked organization - CNO), national hubs and services groups.	Several options are considered for transition from ECHO project to ECHO CNO. Stakeholders Committee plays a role in establishing and maintaining partnerships and	Project outcomes (E-WS, E-FCR, FCSF) are considered as a base for the future service groups. The strategic activities, are guided, discussed, and approved within the units of the

		relations with relevant external stakeholders on each level.	Central Hub, including incubation of new services, innovation events and entrepreneurships education
SPARTA	Strategic Direction, under which there are different committees (e.g., Roadmap Committee, Partnership Committee with its Council of associated partners), task forces (e.g., Training and Awareness Taskforce), boards (security advisory board) and programs (there are four programs and in each one there is a team of stakeholders)	Project established interaction patterns with external stakeholders and level of stakeholdership. However, there are multiple comments [12] reporting uncertainness about the role, function of external stakeholders in general, and associates in particular.	Examples include research roadmaps and "moonshot" initiatives for cyber security research, transversal activities such as certification, training, and social aspects, awareness building and cyber skill development
CONCORDIA	Advisory Board (AB), Ethics Advisory Board (EAB), Management Board (MB), Industrial Strategy Committee (ISC), PPPartnership Board (PPPB), Scientific and Technological Committee (STC), and Security Advisory Board (SAB), but the links between these, or conclusions from the operational piloting of these boards, are not described or reported	Research stakeholders are mainly grouped in WP1, while industrial stakeholders are brought together in pilots and in ISC. CONCORDIA is the only pilot project that has dedicated start-up community of stakeholders.	List of services is published on web page and includes cybersecurity expert advice, skill development, access to tools, start-up guidance, career opportunities etc.

boards or structures in this project, including Advisory Board (AB), Ethics Advisory Board (EAB), Management Board (MB), Industrial Strategy Committee (ISC), PPPartnership Board (PPPB), Scientific and Technological Committee (STC), and Security Advisory Board (SAB), but the links between these, or conclusions from the operational piloting of these boards, are not described or reported yet. ISC, for example, is responsible for the ranking of exploitable results

on annual basis, based on technology readiness level (TRL), innovation potential and the importance of the cybersecurity ecosystem support for the further exploitation. Although this body has a clear industrial bias, as it is composed exclusively from industrial community representatives, it does contribute to a better understanding of EU industrial cybersecurity priorities and better alignment of research and industry. Finally, we also find description of an overall project objective, where it is stated that "CONCORDIA addresses governance model that combines the agility of a start-up with the sustainability of a large center." Indeed, start-ups are both inspiration for the governance in CONCORDIA, as well as one of the targets for the community building.

In October 2021 ENISA, ECSO and four pilot projects (CONCORDIA, SPARTA, CS4EU, ECHO) submitted their draft recommendations to the ECCC, following a consensus process about the future priorities. Besides these recommendations, representatives of these projects and institutions elaborated "concept on the way forward" with 11 strategic directions where "cybersecurity competence community" could make significant contribution. Although four pilot projects have gathered views from more than 80 stakeholders via survey, interviews, and workshops, it is also legitimate to pose a question why not all partners of four projects (more than 160) did not participate in this exercise. This problem of motivation and incentives is even more evident in a recent public consultation of Cyber Resilience Act [40] that closed on May 22nd, 2022.

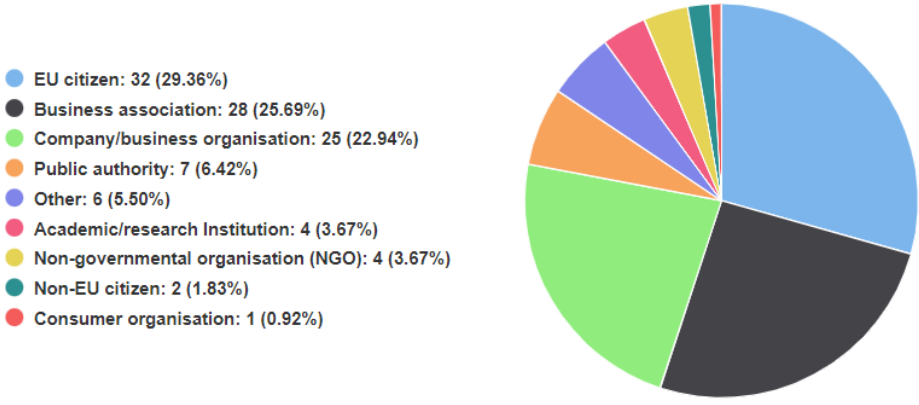

Figure 1: Statistics on CRA public consultation by category of respondent.[40]

Among 109 respondents we can see, in Figure 1, that more EU citizens participated in the consultation than from any other stakeholder group or community category. Although it can be argued that many organizations were indirectly represented by the corresponding community associations, it is still remarkably low number or responses for such an important consultation.

We conclude this chapter with a general observation that, although collaboration and cooperation in all four pilot projects can be analyzed from several per-

spective, from co-design (e.g., road mapping or innovative prototypes) to the service co-delivery (e.g., data sharing and coordinated response from different security teams). In all related processes, norms, rules, or actions (PRNA), there are still many open questions and issues, that should influence governance model evolution for the cybersecurity ecosystem and the CC.

On Networks and Ecosystems: Learning from the Other experiences

Networks, their behaviour, evolution, or effects on joint value have been studied in many contexts. Depending on these contexts, the added value that benefits nodes (communities, organizations, and persons) in these networks, depends on the openness and the level of centralization (see for example [41]). Some properties of networks that have been studied, in relation to their performance or value creation, are randomness, heterogeneity or modularity. It is widely accepted that hierarchic networks are more suitable for objective and strategy setting, while distributed networks excel in innovation.

Homophily describes tendency of individuals to associate with similar others, and it has been described in many network studies.[71] Links within “archipelagos” or community clusters are so called “strong” links, while links with outside nodes are often neglected in governance models. Yet, these “weak” links, sometimes even at a personal level, are sometimes more important or relevant for the community building, compared to strong institutional links.

Another lesson from network theory is related to a tendency of distributed community-based networks to turn over time into more fixed and conservative hierarchies, while at the same time new “peer-to-peer” community structures start to appear from bottom-up. This might be inevitable, but the dynamicity of network behaviours should be acknowledged with the evolution of hybrid governance models.

In network science, there is also something called “Matthew effect” [42] that is used to describe the preferential attachment, basically that a node that acquires more connections will increase further its connectivity at a higher rate. It is a kind of accumulated advantage. Unwritten rule that "the rich gets richer, and the poor get poorer" can be sometimes observed, for example, also in EU-funded research projects. EFFECTS+ project, which was a coordination and support action financed by the EC in FP7 program, delivered a report [43] presenting the innovation potential of FP7 Security and Trust projects.

An interesting finding (see Figure 2) was that in community of EC-funded FP7 projects there are few nodes, represented by large software companies and IT integrators (such as IBM, SAP and ATOS), which act as hubs for the other project partners in the R&D community. This can be easily explained by their size and importance for the community, but if we look at datasets beyond FP7, we are likely to find also smaller and less known companies acting as a hub, something to be attributed to “Matthew effect.” It could be good to compare “national cybersecurity R&D networks” and “network of EU-funded project partners” to check whether these show considerable differences, as well as to monitor evolution of these networks throughout EU programs.

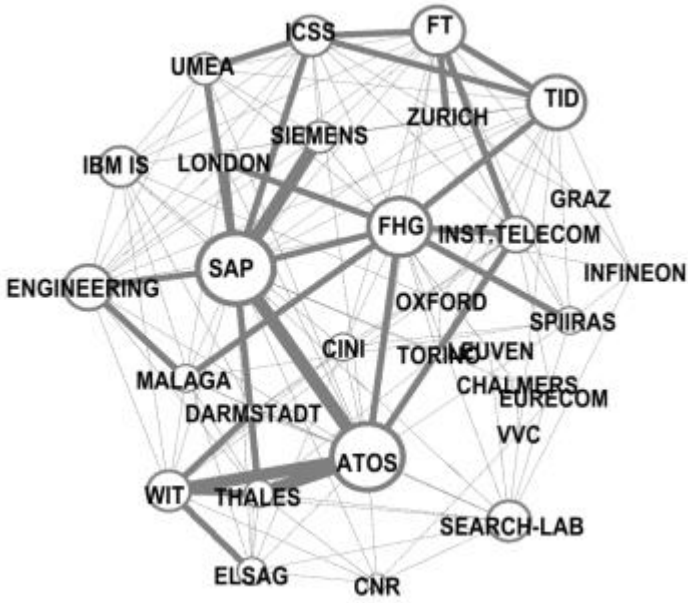

Figure 2: Social relationship graph in trust and security projects in FP7 Call 5.[43]

Why these things matter? As we saw in the previous chapter, there is an ongoing discussion what role should European Cybersecurity Competence Centre (ECCC) and National Coordination Centers (NCCs) play in the future CC membership "gatekeeping," financing and other processes. Let us analyse two alternatives:

a) CC members interested in R&D funding collaborate at EU level, and talk directly to ECCC (basically as it happens now in Horizon Europe with DG CNECT)

b) CC members collaborate at national level, form mini-partnerships or clusters, and then apply for R&D funding together with the other mini-partnerships from few member states (an example could be Eureka Clusters that had thematic funding programs such as ITEA, CELTIC and others.[44]

One can argue that both approaches have pro and contra. EUREKA projects have witnessed, decentralized funding for R&D projects is posing serious risks to synchronization of activities across EU. Some of those projects underperformed due to the isolation of activities in member state (MS) partnerships, and delays in national funding.

EU partnerships and consortia on per-partner basis enable organizations to work directly together with the best or most suitable partners, no matter where

this partner is based. While this might work well for the academics and large industry, for the community of end users' proximity could be an important requirement, as there are many other services (deployment, training, maintenance) needed after the project ends, to make research results transferable to operational environments. In addition, many smaller entities have it more difficult to get access to EU-funded projects and networks. These are sometimes represented, at EU project level, by associations or "business ecosystems" [45, 46] understood here as structures around which large companies co-evolve their skills together with academic partners and smaller, more agile companies.

A related concept is also digital business ecosystem (DBE), defined as "a collaborative environment made up of different entities that co-create value through information and communication technologies (ICTs)." [49] It has been developed in the context of the implementation of the eEurope 2002 action plan (and projects funded by the 6th Framework Programme of the European Commission). The main characteristics of DBEs are platform, symbiosis, co-evolution, and self-organisation.[50]

While these structures, as well as similar "triple helix" [47] and even "quadruple and quintuple helix" [48] support cooperative innovation models, all build upon idea that value creation is done by putting together different assets and skills, we must acknowledge that cybersecurity is not "business as usual." Differences exist, for example, in complexity of digital supply chain, role of supply side partners, the "moving target" issues and others. Cybersecurity spans not only technology, but also people and processes. Cybersecurity is a journey, not a destination. Besides, CC structures need to address not only innovation processes, but also others, such as management of capacity building resources ranging from federated cyber-range platforms to research testbeds.

A report focusing on the governance model of the Hague Security Delta (HASD) also brings forward interesting observations.[62] Lack of hierarchy between the collaborating partners require specific agreements and mechanisms of coordination, as well as the willingness of the parties involved to give up, at some stage, total control of the process and results. Differences can be a source of strength (complementarity, heterogeneity …), but lead to disruption and conflict. The authors focus only on collaboration of a temporary nature. Still, more importantly, they analyze co-existence of hierarchical lines set out by government bodies with what is seen as a "networked" model. In Figure 3 they depict possible interplay between two governance models.

Finally, if we look for more good practices and examples of network behaviors at EU level and innovative ideas for governance models, we might look at European Blockchain Partnership (EBP) and European Blockchain Services Infrastructure (EBSI) that was started in 2018 by 29 countries (All EU Member States, Norway and Lichtenstein) and the European Commission.[51] The list of members is public, as well as its structure or membership in some groups (e.g., usergroup). Financing is assured by the Connecting Europe Facility (CEF), initially, and the new Digital Europe Programme (DEP), from 2021. When it comes to

decision bodies and detailed set of implementation agreements, these are still to be defined, as it is suggested by the "legal track of EBSI."

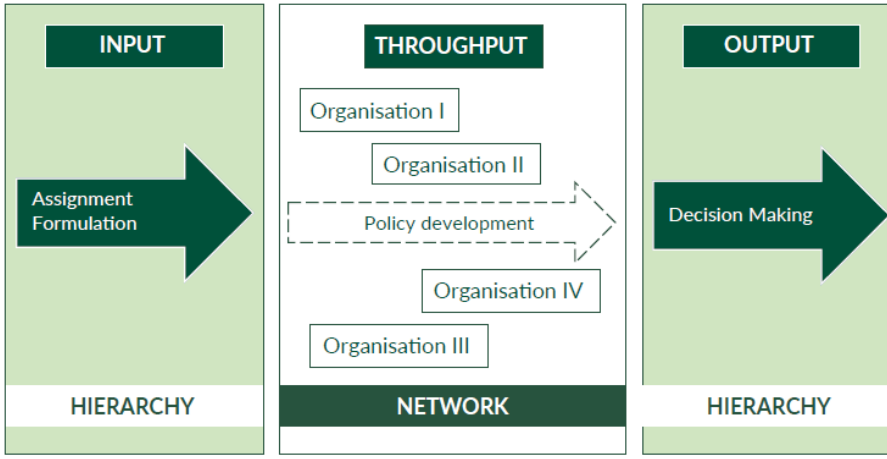

Figure 3: Legitimacy and the decision-making process in a triple helix collaboration.[63]

The core service platform currently in place for EBSI is procured with European Commission DG DIGIT. The Commission services are also working on formal agreements for the future relationships between different stakeholders (EBSI Consortium, between the Consortium and node operators, or the Consortium and application service providers that operate Use Cases). Within community, it has also been suggested that these might use Multi-Country Projects (MCPs) instrument, part of EC proposal for the 2030 Policy Programme "Path to the Digital Decade." This is a strategic governance tool to ensure coherence and synergies among different initiatives, actions, measures, and investments. The Commission also analyzed EBSI as concrete case study to assess the need for a new instrument, European Digital Infrastructure Consortium (EDIC), that would address implementation features of MCPs.

What is particularly interesting in the case of EBSI, is the role of the European Blockchain Association (EBA) [52] and similar representatives of "blockchain community." This organization is structured as a Decentralised Semi-Autonomous Organisation (DSAO), which is derivative of the original Decentralised Autonomous Organisation (DAO), describing a type of network connecting individual nodes that act autonomously with self-created rules.

DAO governance model is described as "the future of meritocracy models," although some call it "algocracy" (ruled by an algorithm). Procedures, such as decision making, use tokens that grant voting powers, and tokens are earned in a different way ("proof of value" for the contribution to the community could be used, for example). Governance is based on a series of proposals that members vote on through the blockchain, and the possession of more governance tokens often translates to greater voting power. Contributions can be tracked and compensated. It might be an interesting experiment in the future of the CC,

for example, in setting the priority for strategic cybersecurity research, evaluation and selection of the new projects, or in the process of ranking of exploitable result from EU projects.

Going for Hybrid: Governance Mesh

There will be no "silver bullet" or "one size fits all" approach, when it comes to EU member state cybersecurity community building and evolution. Some MS will start (or have already started) from the existing well-recognized cybersecurity hubs, communities, or stakeholder groups, while others will strive to merge and converge several (often regional or sectorial) initiatives. Few MS might have to start from scratch. As we have seen from above, both top-down and bottom-up, as well as centralized versus decentralized approaches, have their pro and contra and should be applied on "per process" basis. This analysis should cover three governance model pillars:

- Who: list of relevant stakeholders?
- What: list of processes, rules, norms, and actions (PRNA) with a different degree of formality?
- How: list of parameters (cost, desirability, suitability etc.) to decide about the most suitable governance model options?

The question "who," roughly describes stakeholders, without need to go into detail of balanced distribution of control, or exact decision-making processes between centralized (EC) and decentralized (member states, community hubs) organizations. The second question is about "what" and should start with the analysis of any Processes, Rules, Norms, and Actions (PRNA), that are included or linked to fundamental areas already identified in four pilot projects (e.g., capacity building, incident response, R&D management etc.). Here, those PRNA that refer to high level objectives and strategic goals should follow top-down approach, treated as the strategic governance model issues, while operational layer PRNA might need to have an additional NCC mapping of roles and actions, as well as additional space for inclusion of bottom-up observations and feedbacks.

Finally, the third issue to tackle in a hypothetic hybrid governance model, is question of "how," namely the list of parameters and indicators, such as cost, desirability, feasibility, and suitability, that would help not only in implementation, but also in monitoring and evolution of the governance model.

One of the most important, but also the most difficult features, that is crossing all three pillars of governance (who, what and how), is dynamicity, as the ecosystem and community need to continuously adapt and respond to technology push and market pull forces (see Figure 4). There is always a threat, and even more in cybersecurity, that governance model with static structures or procedures could become obsolete rapidly. We can even see this in EU R&D projects that often last for 3 or 4 years, and do not have flexibility built-in by

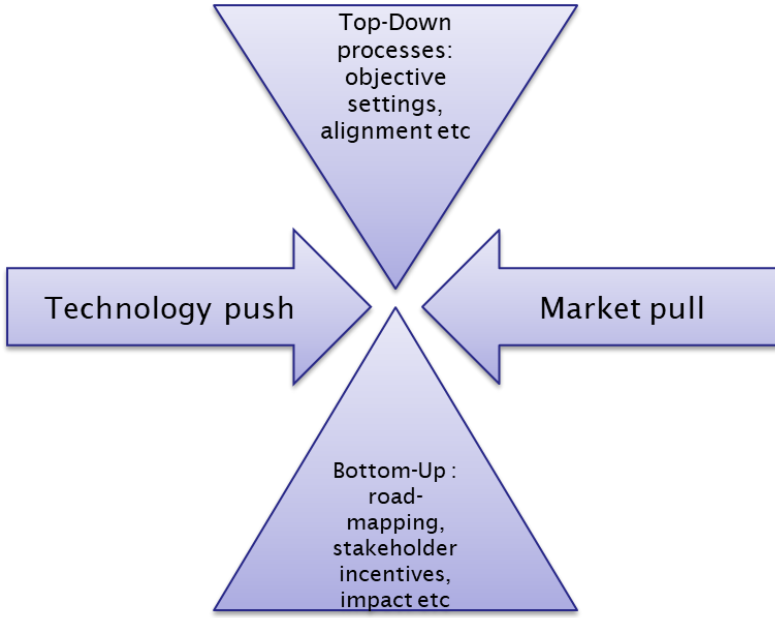

Figure 4: Hybrid governance model that also considers innovation ecosystem forces.

design. In so called Boyd loop (also called OODA loop [66] due to its cycle observe–orient–decide–act), all decisions are based on observations of the evolving situation with procedures in place to make rapid assessment, filtering, or prioritization of the problem being addressed. Continuous monitoring of performance, frequent assessment of substructures and their results and update of governance model, should make it less fragile and prepared to deal with uncertainty.

So, having these observations in mind, what kind of a hybrid governance can we model, if only at a very abstract and theoretical level?

Cybersecurity Mesh Architecture (CSMA) is an architectural approach proposed by Gartner [70] that promotes interoperability, more consolidated security posture, reduction of operational complexity, cost saving, and integration with a broad ecosystem of technologies and vendors. Inspire by this trend, we propose a concept of “governance mesh” model that takes the best of each four pilot projects, enhanced with the other external contributions. It should also acknowledge lessons learned from the previous and related initiatives, as well as the further analysis of PRNA that needs to take place in this emerging cybersecurity ecosystem.

We should also have in mind Linus's law,[35] named in honor of Linus Torvalds, creator of Linux operating system: "given enough eyeballs, all bugs are shallow." EC or ECCC consultations, but also other calls for actions, e.g., data sharing, should be frequent, better advertised, incentivized, and associated with some kudos or credits for the most valuable contributions, according to the community judgements.

Collective intelligence (CI) emerges from the collaboration, but also from competition. It may involve formal consensus between communities or stakeholders, but we should not ignore informal chats with new insights. Link between personal networks, and ways of processing information (e.g., road mapping, cybersecurity intelligence sharing, capacity building), is not always straightforward and is not always easy to capture in PRNA, templates, guidelines, or frameworks. Some degree of "randomness" or improvisation or brainstorming is needed, with a stage/gate model that could filter and rank the best ideas and move them forward.

Everyone agrees that cybersecurity is a problem larger than one sector or one country, but also larger than EU. The cooperation with countries outside EU is not a choice, but rather a must for the EU cybersecurity ecosystem. Scientific Advice Mechanism (SAM) High Level Group (HLG) strongly recommends in their report [61] that the EU should play a more prominent role in establishing effective cybersecurity governance globally. However, this cooperation comes in various combinations and at different levels: member state, organizational and individual, sometimes also related to the pre-existing relationships and trust, which serves as an anchor of all cooperation and collaboration. In a feasibility study,[55] we described other forms of existing international cooperation in cybersecurity, and more good practices and lessons can also be taken from 2021 EUISS report.[56]

Governance "mesh" must live and cope with an apparent paradox: while there is a global inter-dependency in cyber defense and need for the collaboration at a global scale, EU cybersecurity ecosystem must also rely on national and regional actors, and links to the smallest local SME, in order to really have an impact. From strategic to operational level, global to local, many sub-networks, cross-communities, and infra-clusters will feed the overall structure that evolves and adapts over time.

Conclusions

Cybersecurity ecosystem modelling is a topic of particular importance for the future EU cybersecurity policy, as it links EU Cybersecurity Competence Centre (ECCC) and Network of National Coordination Centres (NCCs), with the activities of Cybersecurity Community (CC). In this respect, four pilot projects of cybersecurity competence community (ECHO, SPARTA, CSEU and CONCORDIA) have already provided inputs and feedback on several issues, including governance model, strategic directions, gaps, and challenges. Pilot projects came with few recommendations, such as Community Hubs of Expertise in Cybersecurity Knowledge (CHECKs), or Collaborative Networked Organisations (CNOs). Some member states, in parallel, already started with NCC and consolidation of the existing communities around them, or even building of the new ones. However, formal acknowledgement of these "community hubs," as well as the role and integration of CC into the overall ecosystem governance, is still an open issue.

We have also presented some other "ecosystem"-like initiatives, not necessarily limited to cybersecurity. They are characterized by an idea of value creation by putting together different assets and skills, and they all give insight on how communities, organizations and persons behave in an ecosystem. Too much top-down governance, and they will lose motivation and interest. Too many bottom-up discussions and they lose time and focus.

We introduce "governance mesh" concept, with "community of networks" (e.g., network of NCCs) and network of communities (e.g., network of community hubs in CC), that both need to evolve and monitor their contribution and effects on a joint value. Centralization versus decentralization and top-down versus bottom-up approaches are the main axis for analysis of Governance Processes, Rules, Norms, and Actions (PRNA). Beyond balancing of "technology pull with market pull," important for the dynamics of model, there is also a further need to improve policy-market-technology-society alignment. Gaps might appear in territorial coverage, capacity, and maturity, while dynamics of relationships might have a direct impact on trust.

Shaping Processes, Rules, Norms, and Actions (PRNA), that are included or linked to the fundamental areas already identified (e.g., capacity building, incident response, R&D management, etc.), still needs to find place. Inclusion of specific governance sub-models for specific areas (capacity building, incident response, R&D etc) might also help, as well as addressing PRNA for the horizontal services. This also holds for the specific instruments or processes that aim to reduce gaps between research and market or enabling mapping between demand and supply. The economic impact attribution to "ecosystem existence" will be hard to validate, but governance model must include parameters and indicators that enables its continuous monitoring, also in economic terms.

Links to international stakeholders are also essential, and so are links to open-source and other related EU communities in digital technologies (e.g., GAIA-X, DAIRO, FIWARE, AIOTI, different DIHs, etc.). Assessment of these "external" links is yet to be done. Standardization and certification bodies, individual investors, business angels, public administration, incubators, accelerators, innovation centers, professional associations of cybersecurity practitioners, citizens, and others should also become involved.

Acknowledgements

This paper is supported by European Union's Horizon 2020 research and innovation programme under grant agreement No 830929, project Cybersecurity4Europe, and grant agreement No 830927 project CONCORDIA (Cyber security cOmpeteNce fOr Research anD Innovation).

References

1. European Commission, "The Cybersecurity Strategy," 2022, https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy.

2. European Commission, "European Cybersecurity Competence Network and Centre," 2022, https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-competence-centre.
3. "Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres," Document 32021R0887, 2021, https://eur-lex.europa.eu/eli/reg/2021/887/oj.
4. European Cyber Competence Network, Joint web site for four pilot projects of cybersecurity competence community, 2022, https://cybercompetence network.eu/.
5. Oxford Learner's Dictionaries, 2022, https://www.oxfordlearnersdictionaries.com/
6. Guido Caldarelli and Michele Catanzaro, *Networks: A Very Short Introduction* (Oxford University Press, 2012).
7. "ISO/IEC 27032:2012 Information technology — Security techniques — Guidelines for cybersecurity," 2022, https://www.iso.org/standard/44375.html.
8. Igor Nai Fovino, Ricardo Neisse, Alessandro Lazari, Gian-Luigi Ruzzante, Nineta Polemi, and Malgorzata Figwer, "European Cybersecurity Centres of Expertise Map, Definitions and Taxonomy," JRC technical report, 2018, https://publications. jrc.ec.europa.eu/repository/handle/JRC111441.
9. "CONCORDIA: Project deliverable D6.3. Innovation management strategy," 2020, https://www.concordia-h2020.eu/.
10. "ECHO: Project deliverable D3.2. Governance alternatives," 2020, https://echonet work.eu/.
11. "Cybersecurity4Europe: Deliverable D2.2. Internal Validation of Governance Structure," 2020, https://cybersec4europe.eu/.
12. "SPARTA: Deliverable D1.2. Lessons learned from internally assessing a CCN pilot," 2020, https://www.sparta.eu/.
13. ECSO web page, 2022, https://ecs-org.eu/.
14. Cybersecurity cPPP web page, 2022, https://ecs-org.eu/cppp.
15. EOS web page, 2022, http://www.eos-eu.com/.
16. ASD web page, 2022, https://asd-europe.org/.
17. European Community of CISOs announcement, 2022, https://ecs-org.eu/ news-room/discover-ecsos-first-ever-european-community-of-cisos.
18. "Four Years of Pan-European Public Private Cooperation," EP3R 2010-2013, ENISA report, November 2014.
19. Aljosa Pasic, "NESSI and ESFORS: Paving the way towards secure software services," European Critical Information Infrastructure Newsletter, October 2006.
20. Aljosa Pasic, *Building blocks for Future Internet of Services: Trust, Security, Privacy and Dependability* (MIT Press book on New Architectures for Future Internet, 2009).
21. "Good Practice Guide on Cooperative Models for Effective PPPs," ENISA report, October 2011.

22. European Commission, "Guidelines for Successful Public Private Partnerships," March 2003, https://ec.europa.eu/regional_policy/sources/docgener/guides/ppp_en.pdf.
23. "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace," JOIN/2013/01 final, 2013, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52013JC0001.
24. Trust in Digital Life, 2022, https://trustindigitallife.eu/.
25. ENISA, *Public-Private Partnership (PPP): Cooperative Models* (Information Sharing and Analysis Centers (ISACs), 2018), https://op.europa.eu/en/publication-detail/-/publication/597dee0f-2285-11e8-ac73-01aa75ed71a1.
26. Network of Excellence on Engineering Secure Future Internet Software Services and Systems (NESSOS), 2022, http://www.nessos-project.eu/.
27. European Network of Excellence in Cryptology - Phase II, 2022, https://cordis.europa.eu/project/id/216676.
28. Cyber Competence Network – joint web site for four pilot projects of cybersecurity competence community, 2022, https://cybercompetencenetwork.eu/.
29. Cybersecurity4Europe "Project deliverable D2.1. Governance Structure v1.0," 2020, https://cybersec4europe.eu/.
30. "Digitising European Industry Imitative Report," Working Group 2, Digital Industrial Platforms, August 2017.
31. "DIHNET.EU – project deliverable: Defining Digital Innovation Hubs as part of the European DIH network," April 2020, https://dihnet.eu/.
32. JRC technical reports, "Digital Innovation Hubs in Smart Specialisation Strategies, Early lessons from European regions," 2018, https://publications.jrc.ec.europa.eu/repository/handle/JRC113111.
33. "ECHO project deliverables, D3.2: Governance Alternatives, D3.4: Governance implementation plan," 2020, https://echonetwork.eu/.
34. COBIT framework web page, https://www.isaca.org/resources/cobit.
35. Eric S. Raymond, *The Cathedral and the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary* (O'Reilly, 1999).
36. "SPARTA: Deliverable D1.2. Lessons learned from internally assessing a CCN pilot," February 2020, https://www.sparta.eu/assets/deliverables/SPARTA-D1.2-Lessons-learned-from-internally-assessing-a-CCN-pilot-PU-M12.pdf.
37. SPARTA – Innovation governance blog entry, 2022, https://www.l3ce.eu/en/innovation-governance-based-on-the-diversity-of-factors-that-shaped-the-development-of-the-sparta-t-shark-program/.
38. "CONCORDIA: Newsletters," 2020, https://www.concordia-h2020.eu/concordia-service-cybersecurity-updates/.
39. "CONCORDIA: Deliverable D5.4: 3rd year report on exploitation, dissemination, certification and standardization," 2020, https://www.concordia-h2020.eu/deliverables/.

40. "Cyber resilience act – new cybersecurity rules for digital products and ancillary services," 2022, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13410-Cyber-resilience-act-new-cybersecurity-rules-for-digital-products-and-ancillary-services_en.
41. Jari Arkko "The influence of internet architecture on centralised versus distributed internet services," *Journal of Cyber Policy* 5, no. 1 (2020): 30-45, https://doi.org/10.1080/23738871.2020.1740753.
42. Daniel Rigney, *The Matthew effect: How advantage begets further advantage* (New York: Columbia University Press, 2010).
43. Fabio Massacci, Martina De Gramatica, and Olga Gadyatskaya, "The Innovation Potential of FP7 ICT Trust and Security Projects," Executive summary and policy paper, Effects+ project, March 2013 https://securitylab.disi.unitn.it/lib/exe/fetch.php?media=whitepapers:innovationpotentialofeusecurityprojects.pdf.
44. EUREKA – public network for international cooperation in R&D, 2022, https://www.eurekanetwork.org/.
45. Elisa Anggraeni, Erik Hartigh, and Marc Zegveld, "Business ecosystem as a perspective for studying the relations between firms and their business networks," Project: Business ecosystems, 2007.
46. Simon Wieninger, Rafael Götzen, Gerhard Gudergan, and Kai Wenning, "The strategic analysis of business ecosystems: New conception and practical application of a research approach," *2019 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC), Valbonne Sophia-Antipolis, France*, 2019, pp. 1-8, https://doi.org/10.1109/ICE.2019.8792657.
47. Henry Etzkowitz, *The triple helix: University-industry-government innovation in action* (New York: Routledge, 2008).
48. Elias G. Carayannis, Thorsten D.Barth, and David F. J.Campbell, "The Quintuple Helix innovation model: global warming as a challenge and driver for innovation," *Journal of Innovation and Entrepreneurship* 1 (2012).
49. F. Nachira, P. Dini, and A. Nicolai, "A network of digital business ecosystems for Europe: Roots, processes and perspectives. Digital business ecosystem," European Commission Information Society and Media, 2007.
50. Prince Kwame Senyo, Kecheng Liu, Lily Sun, and John Effah, "Evolution of norms in the emergence of digital business ecosystems," In: M. Baranauskas, K. Liu, L. Sun, V. Neris, R. Bonacin, & K. Nakata (Eds.), *Socially aware organisations and technologies. Impact and challenges* (2016), 79–84.
51. European Blockchain Services Infrastructure (EBSI) - web page, 2022, https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Home.
52. The European Blockchain Association (EBA), 2022, https://europeanblockchainassociation.org/.
53. Usman W. Chohan, "The Decentralized Autonomous Organization and Governance Issues," Regulation of Financial Institutions Journal, *Social Science Research Network*, 2017.

54. "Strategic Research Agenda of Network and Information Security (NIS) Platform," October 2014.
55. "Feasibility Study on The Establishment of The World Bank-Korea Cybersecurity Center for Development," Atos report for The World Bank, 2014.
56. Robert Collett, Nayia Barmpaliou, and Patryk Pawl "International Cyber Capacity Building: Global Trends and Scenarios," EUISS report, 23 September 2021, https://www.iss.europa.eu/content/international-cyber-capacity-building-global-trends-and-scenarios.
57. "SECCORD project: Deliverable 6.2. Identification of Future Emerging Issues/Topics," 2015, https://cordis.europa.eu/project/id/316622.
58. "SECCORD: Deliverable 5.5. Catalogue Year 3," 2015, https://cordis.europa.eu/project/id/316622.
59. Julián Seseña and Diego Soro, "The National Technology Platforms," 2021, https://www.academia.edu/213168/The_National_Technology_Platforms.
60. "NIS platform: Business Cases and Innovation Paths," 2014, https://cybercamp.es/cybercamp2015/sites/default/files/contenidos/material/2_cybercamp_nis_wg3_sra.pdf.
61. High Level Group of Scientific Advisors, "Cybersecurity in the EU Digital Single Market," 2017.
62. Richard Franken, "The Hague Security Delta: The Dutch Method of Collaboration and Innovation for Security," *European Cybersecurity Market*, 1, no. 4 (2017).
63. Maurits Sanders, "Werk in Uitvoering, Legitieme besluitvorming door PPS" *Recht der Werkelijkheid* 31 (2010), [Work in Progress, Legitimate decision-making by *PPS, Reality rules* 31 (2010)].
64. Aljosa Pasic, *Research-to-market transition in European cybersecurity projects*, 1st edition (Leon: Jornadas Nacionales de Investigación en Ciberseguridad (JNIC), 2015).
65. ENISA, "EU Member States Incident Response Development Status Report," 2019.
66. John R. Boyd, "Destruction and Creation," U.S. Army Command and General Staff College, 1976.
67. "Addressing the innovation gap: Lessons from the Stairway to Excellence (S2E) project," JRC Report, 2018.
68. "Cybersecurity4Europe: deliverable D06.1 Case Pilot for WP2 Governance," 2020, https://cybersec4europe.eu/.
69. European Innovation Council (EIC) "Work Programme 2022," https://eic.ec.europa.eu/eic-funding-opportunities/eic-pathfinder_en#eic-work-programme-2022.
70. "Top Strategic Technology Trends for 2022: Cybersecurity Mesh," Gartner report, October 2021.
71. Miller McPherson, Lynn Smith-Lovin, and James M Cook, "Birds of a Feather: Homophily in Social Networks," *Annual Review of Sociology* 27 (2001): 415–444, https://doi.org/10.1146/annurev.soc.27.1.415.

About the Author

Aljosa Pasic graduated in Information Technology at the Electrotechnical Faculty of Technical University Eindhoven, The Netherlands, and worked for Cap Gemini (Utrecht, The Netherlands) until the end of 1998. In 1999 he moved to Sema Group (now part of Atos), where he occupied different positions. During this period, he participated in more than 70 international research, innovation, or consulting projects in information security. He regularly collaborates with various international organisations and has been a frequent speaker at major international conferences. Currently, he works on several EU projects, such as CONCORDIA or Cybersecurity4Europe.
https://orcid.org/0000-0003-0150-5732