Governance Challenges for European CyberSecurity Policies: Stakeholders Views

Pierantonia Sterlini, Fabio Massacci
University of Trento, Italy

Natalia Kadenko, Tobias Fiebig, Michel van Eeten
Technical University of Delft, The Netherlands

Abstract— We outline possible approaches to cybersecurity governance and compare them against the EU proposal of a Network of Competence Centers, which should manage all European cybersecurity funding. We test such policy proposal against the opinions of key stakeholders (senior administrators from European Agencies, Data Protection Authorities, CISOs, managers, and academics).

Index Terms—policy, security, law, economics, security management, research and development management, innovation management, technology management

1 INTRODUCTION

SECURITY issues affecting private data of millions of citizens, organizations trying to influence elections, and state actors attacking critical infrastructures made cybersecurity a focus of policy makers. Cybersecurity governance is now part of trade negotiations along traditional issues such as tariffs on cars, as in the negotiations between the EU and the US on conformity assessment [1].

Yet, when trying to create governance frameworks for cybersecurity, policy makers often lack "user requirements". Proposing more (or less) centralized regulation can always be done but it may not be the most effective option[3]. Indeed, the diverse, distributed, evolving, and global nature of cyber threats often requires responses stemming from coordinated partnerships. Therefore, when deciding whether to prioritize research or skills development—policy makers need a ground-truth on the needs of existing stakeholders to avoid impractical frameworks that may hinders existing collaborations.

For example, the Atlantic Council report on cybersecurity [4] recommends a "state-centric cybersecurity expert center" in the US as a part of a new governance model. It also mentions "organizing around like-minded countries", i.e. intensifying international cooperation and conducting joint campaigns in response to cyber threats.

Similarly, the European Commission (EC) has proposed to introduce a Cyber Security Competence Center and Network of National Centers (for short Cyber *C&N*) in charge of the EU financing of cybersecurity R&D. The legislative process has broadened its scope, for example to include professional education. The Cyber C&N is an interesting case study for cybersecurity governance given the wide diversity of involved stakeholders (from government officials to hacktivists). We are interested in understanding how these groups see their role and what they think is the final goal the Cyber C&N should reach.

The core of our contribution is the analysis and the empirical validation of different models of cybersecurity governance for the Cyber C&N to inform the EC and EU Parliament decision-making process. We seek to elicit three research questions from theory, legislative proposals, and direct opinions of European stakeholders to see whether they are aligned:

- RQ1 (**narrow or broad focus**): Do stakeholders envisage a focus on R&D or in broader goals (e.g. professional skills or transfer to market)?
- RQ2: (**decision making**) What governance framework structure do they think will stimulate their target cybersecurity capabilities?
- RQ3 (**key players**): What key organizations they want to leverage and rely on for such EU wide cyber security competence network?

To answer these questions, we first discuss several models of governance and how the legislative initiative of the EU on the Cyber *C&N* fits these models. We then conduct a quantitative and qualitative study with key EU stakeholders to collect their opinions

- *Pierantonia Sterlini and Fabio Massacci. DISI, University of Trento, Via Sommarive 5, 38123 Italy. E-mail: {p.sterlini, fabio.massacci}@unitn.it.*
- *Natalia Kadenko, Tobias Fiebig, and Michel van Eeten: TPM, TUDelft, Jaffalaan 5, 2628 BX Delft, The Netherlands. E-mail {n.i.kadenko, t.fiebig, m.j.g.vaneeten}@tudelft.nl*

(CISOs from Fortune 50 companies, senior officers from EU Agencies and Data Protection Authorities, industry managers, hacktivists, and academics). Our findings shed light on the key issues that policy makers should address when designing a governance model for cybersecurity.

2 GOVERNING CYBERSECURITY?

There is not one-size-fit-all model for governance. In his classic work Powell [4] discusses three governance models: *market, hierarchy, and network*.

When it comes to cybersecurity, the invisible hand of the *market* is showing itself openly, world failures included [5]. Within this model, the economic exchange largely preserves the autonomy of the actors whose costs and benefits are self-assessed (e.g. software cost vs. cost of possible data loss), and no long-term feeling of trust and obligation emerges. Where overarching governing approach of national bodies is lacking, market mechanisms step in to address immediate needs. We can expect market-based stakeholders to ask the Cyber C&N for R&D solutions, since cyber threats have the potential to undermine their profits (i.e. narrow focus in RQ1). Stakeholders favoring the market model would likely prefer a decision-making process that would grant limited powers to the EU body (RQ2). Industry players would likely be named as key stakeholders (RQ3).

The *hierarchical model*, with its rigid vertical, clear task distribution, and bureaucratic rules, according to Powell [4], is suited for high-speed mass production, replacing the uncertainty of market mechanisms with stability and predictability. The backside of stability is lack of flexibility to react to changes, let alone to anticipate them. Desire of predictability may nudge actors toward compliance and 'box ticking' instead of proper risk analysis[2]. Unfortunately, for reacting to rapidly shifting cybersecurity environment, flexibility may be crucial. Hierarchical organizations also require a back up of joint resource pool to safeguard for inevitable insufficient responses. Yet, the requests for additional resources by cyber security ``defenders'' is always vulnerable to threat inflations by what US President Eisenhower called the military-industrial complex and for which robust evidence exists in the cyber domain [6]. The hardest challenge is that this model requires the commitment of a large group of actors, including not just industries and consumers, but representatives of national and supranational political bodies, as well as civil society groups to abide by the hierarchical organization. This model offers space for broader goals, which can be reflected in stakeholders' expressing desire for broader focus (RQ1). The EC would likely be named to get the primary decision-making power (RQ2). Stakeholders may also require involving multiple parties rather than letting industry alone to settle the rules of the game (RQ3).

An alternative to realize a "cyber moonshot" is to consider the cooperative framework of what started out as an institutional moonshot of sorts – and namely the EU. A model of international cyber security cooperation may answer the challenges of cyber security policy-making, similarly to the way that the EU prototypes were the answer to the challenges of peace building in post-war Europe. A common European goal may be best realized in the *network governance model* as described by Powell – "interdebtedness and reliance over the long haul" [4]. A successful network model facilitates the exchange of data and knowledge, for which an environment of trust and the feeling of being united is essential. Pupillo [7] also mentions that "trust-based relationships are essential to cyber security and resilience policy", elaborating on the inherent contradictory market incentives (private costs vs shared benefits). In other words, leaving cyber security to market-based relationships will likely fail to create the conditions necessary for efficient global responses, while hierarchical structures with the clear boundaries of specialization and authority may be inadequate for the challenge of a dynamic environment. The stakeholders' answers indicating preference for the network model would include the need to tackle broad, ambitious cyber security goals (RQ1), by opting for the decision-making process based on consensus and involving multiple stakeholders (RQ2, RQ3). The network model is not immune to challenges, such as perceived loss of independence, unclear responsibilities, and encapsulation. Like many domains that require intense and timely cooperation, it should avoid falling into a state of disequilibrium by producing short-term solutions and sacrificing long-term stability for immediate political gains [8]. Collaborative governance, i.e., "attempts to bring all relevant stakeholders together for face-to-face discussions during which policies are developed" [9] will help tackle additional challenges, such as attracting talent, incorporating relevant input from diverse stakeholders and ensuring sustainable development.

3 EU CYBERSECURITY POLICY

How the Cyber C&N real-life legislative process has realized these governance challenges?

Policy-makers often find it a challenge to write about EU policies without mentioning a "patchwork approach" [14] and "half-hearted progress" [15]. With the growing body of the policy documents and legislative acts on cyber security, several challenges became apparent. First, the EU-wide issue of maintaining balance between national freedoms and supranational regulations remains problematic, because for cyber threats the distinction between these areas is unclear. From identification of the attacker to developing the most efficient responses, cyber security in-

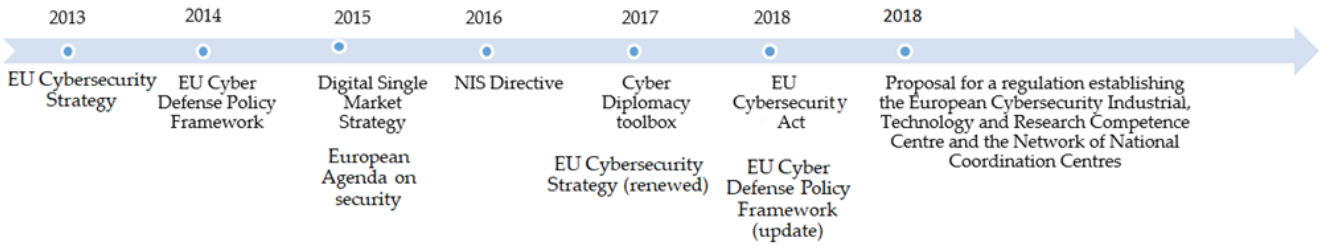

Figure 1 - The Evolution of Europeap CyberSecurity Policy Initiatives

creasingly requires intra- and international cooperation, as well as cross-domain policy responses (e.g. justice, international security and harmonization of education). Additionally, international market forces are an important player in the field.

3.1 The Recent Legislative Evolution

The history of the European cyber security network begins with adopting the Budapest Convention on Cyber Crime in 2001, the Common Framework on Electronic Communications Networks and services in 2002, and subsequent establishing of ENISA, an independent EU Agency for cyber security, in 2004. The main tasks of ENISA were "developing a culture of network and information security for the benefit of citizens, consumers, businesses and public sector organizations in the European Union, thus contributing to the *smooth functioning of the internal market*" (our emphasis) [10]. The model was still the market model with information exchange as a key principle of successful governance.

Figure 2 - The Recent European Policy Initiatives in Cybersecurity

The change in international conditions led to the evolution of the EU Cybersecurity legislation (***Figure 1***). The EU Cybersecurity Strategy from 2013 (updated in 2017) stressed the need for cooperation between Member States, private sector, and EU agencies – ENISA (network), EC3/Europol (law enforcement) and EDA (defense) – to promote awareness of threats, encourage investment, as well as to share best practices [11]. The 2015 European Agenda on Security focused on combatting cybercrime as a key priority through a "coordinated response at European level", including implementation of existing policies and adjusting existing legislation [12]. The 2015 Digital Single Market Strategy pointed to the vital role of investments in novel technologies and support to SMEs. After a number of legislative pieces targeting specific cybercrime issues (e.g. payment fraud), the Directive on Security of Network and Information Systems (the ``NIS Directive'') from 2016 is an example of general EU-wide legislative piece on cyber security. It established the NIS group coordinating strategic cooperation among Member States, providing guidelines for national capabilities, as well as promoting exchange of information. The EU Cyber defense policy framework, adopted in 2014, was updated in 2018 to better correspond to the new challenges [13]. Attention was paid to conflict prevention and cooperation in cyber space, as well as to the availability of information; the updated priorities list included development of cyber defense capabilities, training and exercises, research and technology, civil-military cooperation and international cooperation. The "cyber diplomacy toolbox" from 2017 provided a framework for the joint foreign policy responses to cyberattacks against the EU, to "influence the behavior of potential aggressors in the long term".

On December, 2018, the European Parliament, the Council and the EC reached an agreement on the Cybersecurity Act, which established an EU framework for cyber security certification and granted ENISA additional resources, thus reaffirming ENISA role to support of Member States for cyberattacks management and prevention, as well as in cyber-security policy-making. Whether ENISA was actually successful in fostering this role is debated, as we shall see in the stakeholders' interviews

The evolution path showed the broadening of the goals (RQ1), which have been moving from narrow and market-based to broader and accommodating of the intense cooperation at different levels (RQ2), with diverse stakeholders involved (RQ3) typical for the network model. The political debate also raised the need for stronger cyber security governance at the EU level, in terms of better coordination at operational level, mitigation of operational fragmentation and better resources utilization.

3.2 The Network of Competence Centers

Within this background, the need for a better coordination also of the EU funding of cyber security became apparent as identified by the last steps in Figure 1. On 13 September 2017 a communication from the European Commission was released, entitled "Resilience, deterrence and defense: Building strong cyber security for the EU", which proposed establishing a EU cyber security

competence center with a network of national coordination centers. The initial EC focus was that the Cyber C &N was to coordinate research funding (RQ1).

In December 2018 a rapporteur from the European parliament presented a draft report that stressed the coordinating role of ENISA in the Competence Centre's activities, and called for an advisory role by experts, large and small companies (Hierarchical model - RQ2). The report endorsed a multi-stakeholder approach and the vision of cyber security as a dynamic field that requires a more creative approach than a series of products. [16]

At the time of writing, a "Proposal for a regulation establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centers" passed through the European Parliament. One proposed amendment [17] fits the idea of collaborative governance (Network model - RQ2) by explicitly defining stakeholders as

> "*Industry, public entities and other entities which deal with operational and technical matters in the area of cyber security, as well as to civil society, inter alia trade unions, consumer associations, the Free and Open Source Software community, and the academic and research communities*".

Another amendment addresses capacity (RQ1):

> "*…should deliver cyber security-related financial support from the Horizon Europe and Digital Europe programs, as well as from the European Defense Fund […] the European Regional Development Fund and other programs where appropriate. This approach should contribute to creating synergies and coordinating financial support related to Union initiatives in the field of cyber security research and development, innovation, technology and industrial development and avoiding duplication*".

Amendment 16 was added to address ethical aspects of security and privacy, while Amendment 18 stressed that

> "*The Union needs to be able to adapt fast and continuously to new developments in the field. Hence, the [C&N] and the Cybersecurity Competence Community should be flexible enough to ensure the required reactivity*".

The emerging mixture of hierarchy and network models that is being developed by the EU, while correctly identifying the existing challenges and aiming for transparency, accountability, development potential and resources allocation, may suffers from inefficiency, overlapping competencies, and conflicts of independence. The governance process is further complicated by the nature of the inter-institutional cooperation between EU bodies.

Table 1 – Demographics of Survey Participants

WORK SECTORS OF ALL PARTICIPANTS

Academy	Industry	Regulator, Agency	Trade Association
26	25	3	3

The participants came from 16 Members States of the European Union. Five participants are from non-EU countries. Two of them did not specify their nationality

VERTICAL DOMAINS OF INDUSTRY PARTICIPANTS

Health	Finance.	Incident Reporting	Supply Chain	Smart Cities	Identi Mngt
5	3	4	6	6	9

Multiple answers are possible. Eight participants did not identify a domain. Vertical domains are defined in the call for pilots of the European Union and are essentially close to the business domains from ECSO the European Cybersecurity Organization (an industrial trade organization).

Four pilot projects were launched in 2019, to "assist the EU in defining, testing and establishing the governance model" of the Cyber C&N. Our research was performed in one of them (CyberSec4Europe).

4 COLLECTING STAKEHOLDERS VIEWPOINTS

Various techniques exist for knowledge elicitation [18] but a variant of structured or semi-structured interviews are the most commonly used (See Chapter 42 in [19]). To collect the opinions of stakeholders we took a two-pronged approach as previously done in [20][21]for cyber security policy analysis of stakeholders. A structured survey with over 50 stakeholders to collect suggestions and opinions about the governance model was supplemented by conducting additional 18 P2P interviews based on the notion of "grand tour interviews" [22].

4.1 The Survey

The *survey* included both open questions as well as multiple choices questions to provide a quantitative analysis of the results. The expected time to complete the overall 24 questions was around 15/20 minutes.

The demographics of the stakeholders who responded to the survey are summarized in **Table 1**. The survey has been open for participation from mid-March until the end of August 2019 and made available to the industrial and academic members of the pilots (with an audience of around 200 potential respondents) and 57 completed answers were collected.

TABLE 2 - Demographics from the Stakeholders Interview

ID	*Role*	*Organization*
1	Senior Manager	ENISA
2	Board Member	ENISA
3	Board Member	European Trade Org.
4	Board Member	EU Data Protection Supervisor
5	Senior Manager	European Consumer Org
6	Ethical Hacker	Self-Employed
7	Senior Manager	Semiconductor MNC
8	Vice President	Re-Insurance MNC
9	President	Critical Infrastructure Assoc.
10	CISO	Big Pharma and Energy MNCs
11	Professor	University
12	Policy advisor	Cybersecurity for industry and government
13	Govt. official	National govt., IT Security
14	Professor, entrepreneur	University, small company in security
15	Ethical hacker	Security industry
16	Professor	University
17	Vice President	Software MNC
18	Senior Manager	Financial institution

At the time of writing, the European Cybersecurity Organization agreed to circulate the survey to its members for a major consultation event to take place in November.

4.2 The Interviews

Through a purposive sampling approach [22] we identified some stakeholders to represent a variety of roles specifically involved in cyber security (from agency representatives to data protection authorities, from CISOs to representatives of customers organizations).

For 18 additional stakeholders (**Table 2)** who agreed to be interviewed in persons, we conducted *semi-structured interviews* recorded with participants' permission and transcribed into anonymous form. They were all interviewed in March-June 2019. These interviews allow us to supplement and clarify the findings behind the survey.

4.3 The Questions

Both survey and interviews featured few key questions to elicit answers in a terminology close to stakeholders' own interests. For example, a stakeholder not participating in the Cyber C&N pilots is unlikely to be interested in "generic questions" on governance. However s/he is definitely opinionated on what capabilities Europe should develop and who should be in charge of achieving them (e.g. along the hierarchy or the market model).

Our questions started with the *overall goal in cyber security that Europe should achieve* (e.g. coordination of policies, technological independence, or protection of citizens and state actors from non-EU countries). For example technological independence is a key EU policy issue given the current US protectionist measures (e.g. on Huawei). To achieve this goal we also asked *what should change*?

Then we asked "In your area, *what key capabilities are required* by systems, people, institutions, etc., to achieve that change?" Research and technological innovation were among the options but professional knowledge and skills could also be selected.

With regard to the *key players*, participants were asked to indicate at most 8 players out of a broad list of players (Appendix A). Then we focused on the *decision-making* aspects of the Cyber C&N.

Another hot questions is whether the *Network should push national centers and the industries gravitating around them towards specialization* (i.e. fund a research area only in one Member State). The ``avoiding duplication'' clause in the legislation is often interpreted this way. This is a key question for the USA [3] andother countries opting for distributed network centers (e.g. the UK).

In terms of mandate we asked whether the *Cyber C&N should push towards mandatory security certification at European level*. In the initial EC text there was a provision for identifying areas for mandatory security certification. Industry lobbying effort has weakened the wording: at the time of writing only voluntary certification schemes are considered in the legislative texts.

5 Analysis

In terms of *what should change to improve* the situation (e.g. better resilience, transparency, trustworthiness, security metrics...) respondents considered transparency of cyber security decisions, trust worthiness, and resilience as challenges. Some interviewees [#4, #7, #9, #17] highlighted the need for knowledge and education to be constantly updated to meet the dynamic changes in cyber security: cyber security needs a *new generation of experts of cyber security trained through an*

interdisciplinary approach mastering the security of systems and understanding how cyber security affects the business.

Some participants raised the issue of making sure that the EU taxpayer money in cyber security research through open calls does not benefit US companies through their EU subsidiaries [#1, #3]. In general ***the goal was to achieve cyber-sovereignty, independence, and control*** [#1, #3, #11. #14, #15, #16], clearly expressing preference for the broader focus (RQ1) and indicating support of hierarchical and network models.

The summary on our RQ on focus on technology or on other measures is that ***activities should go beyond funding R&D and include training and innovation***. Indeed, only 32% of the participants to the survey consider the developments of better security technologies as essential and another 35% consider it of major importance. Less than half of them (42%) considered new or improved technical standards of major importance. In contrast, almost half of the respondents consider new professional or academic skills as essential to achieve cyber security capabilities (46%). Also half of them also consider policy interventions of major importance (51%). Interviewees agreed that ***one*** of its objectives was R&D funding [#1, #2, #3, #7, #10] but they also widely diverged on whether it was the only task (as advocated by an EU actor [#2]). For example, three very diverse stakeholders [#3, #6, #10] raised the critical importance, shared by the EU Parliament, of supporting SMEs to bring research to the market, others [#1, #4, #8, #9, #17] focused on professional skills and education. Since all three models are consistent with these opinions, to see ***how*** this should be done we look at other answers.

The certification of infrastructures, service, and products were also indicated as aspects that should change (major importance for a third of respondents). In this respect half of the participants agreed that ***the Cyber C&N should support mandatory security certification***. These answers lean towards hierarchy models.

Among the key questions, the ***quest to specialize research in each national center was not supported by the stakeholders***. Less than a third (28%) supported the option. -A quarter considered it is possible only in special cases, and the rest express a negative opinion. Indeed, the feeling of potential duplication was mostly felt only by stakeholders with a European responsibility (e.g. [#2, #3]) who explicitly mentioned wasted resources). Other stakeholders who saw it as potentially backfiring did not share this view. For example [#4, #6, #10, #17] all identified this policy as effective only in the short term, since it is not possible to predict in advance where new innovation would take place. Others [#4, #10, #11, #12, #13 #16] stated that specialization will occur naturally, and should be capitalized rather than enforced. These answers strongly support the network model and the market model over the hierarchy model.

The majority of the participants consider the European Commission (60%) as a key player as well as ENISA (61%) However almost a fifth (18%) indicated as key player only the EC without considering ENISA. Vice versa, a similar number of respondents (19%) indicated ENISA without mentioning the EC. This can be interpreted as a preference for clear task distribution with the designated structure involved, thus corresponding to the hierarchical model. Still, many stakeholders were not familiar with ENISA. Of those respondents who expressed an opinion, most assigned to ENISA only an "orchestration role", underlining the need of a harmonization between organizations [#17]. Some interviewees [#3, #10] noted that anything effective have not and would not come out to ENISA due to lack of resources.

Most interviewees argued that such decision should be left at Member State levels and that a balance between different stakeholders is desirable. As [#3, #4, #5] observed, different Member States would have different sensibilities and different agencies in charge of national security (e.g. BSI in Germany, ANSSI in France, and DIS in Italy, each referring to a different `kind' of Ministry). Indeed, eventually cyber security will always have a key role for national security and such role is not eliminable by purely considering market issues [#3, #4, #9]. These answers again strongly support the network model.

What emerged as a surprise was the ***role of the Cyber C&N as a first point of contact to support society at large (from SMEs to individual citizens) when seeking cyber security advice***. For example, the majority of the participants (68%) assigned to academia a key role, which is expected for a Center in charge of research funding. Yet, almost a half of respondents pointed to the Computer Emergency Response Teams (CERTs, CSIRTs) to have an advisory role which would be unclear if the activities was limited to just dole out funding for R&D. Several interviewees [#1, #4, #8, #9] highlighted that Cyber C&N could promote mechanisms for sharing of attack data that protects the identification of the victim while allowing other actors to protect themselves. Others also pointed how [#1, #4, #5, #9] normal citizens or ethical hackers could turn to the Cyber C&N for notifying security issues to be passed on to the corresponding regulator of each vertical domain as the company which has the security issues would have clearly a conflict of interest.

Also, more than a half (58%)of the respondents attributed to *Data Protection Authorities* a key role, a proportion comparable to the number selecting the European Commission, thus showing the key important that privacy protection has for European citizens.

6 CONCLUSIONS

From the interviews, ambiguous views emerge of the Cyber C&N. The network of centers works like a projection screen: it is everything to everybody. Stakeholders project on this idea their concerns, interests and ambitions for cybersecurity in Europe. To some extent, this simply reflects the diversity of stakeholders operating in this area. Even the European institutions themselves have laden this policy with a diversity of objectives, hopes and requirements. In reality, it reflect the fact that the policy emerged from a network approach rather than hierarchy.

The complex network governance around the Cyber C&N means that coordination and collaboration will not emerge purely from a shared vision or hierarchically determined structure. In the end, incentives shape what the Cyber C&N will become and deliver. They are the key for policymakers. What will the Cyber C&N and its funding structures reward? International collaboration? Research and development with industry? Products and technologies? Training and education? All of the above?

Concerning first research question, there is no convergence on the relative importance of R&D vs. skill development. Given the diverging viewpoints of our participants, we recommend allocating resources evenly in both directions.

RQ2 has clearly shown a preference for an informed network model (academics) with some elements of hierarchy (EC and ENISA). The presence of CERTs among the stakeholders in charge of advising on funding and education shows the clear importance of incident management in a cyber security governance framework. This is also relevant in terms eventual funding and educational skills should go (which only play a minor role in today's educational charters).

Concerning our third research question, there seems to be a general consensus that the flexibility of the network model seems to be most appropriate to cope with the challenges of cyber security and to provide the flexibility to adapt to the different states economic and policy conditions. Such flexibility also implies that ***there should be no top-down decision on the form for the individual national centers or on their "specialization"***. This has broad consequences also for the Atlantic Council proposal for the US. In terms of operational and decision making rules another broad consensus exists on promoting information sharing about security issues and possibly coming to unifying technical standards about cyber security.

Eventually, if research funding will remain the core of the network finally approved by the EU institutions, the broader ambitions for the Cyber C&N could be accommodated via incentives that reward linking research with societal impacts. The incentive embedded in the funding schemes would strengthen the need for researchers to work with CERTs, industry partners, NGOs et cetera, to improve the actual security of services and solutions in the European Union.

Acknowledgments

We thank A. Ferreira for jointly organizing a survey about the technological roadmap and the governance of the network, S. Fisher-Hubner and P.H. Cros for testing it and all interviewees for their time.

This work has been partly funded by CyberSec4Europe (cybersec4europe.eu) within the European Union's Horizon 2020 programme H2020-SU-ICT-03-2018 under grant agreement No. 830929. The opinions reported in this paper are our own and not necessarily endorsed by the EU nor the organizations of the respondents.

Authors contributions: supervised the research FM, MvE; designed research questions PS, FM, TF; collected data PS, NK, FM; wrote the article FM, NK, PS, TF, MvE.

7 REFERENCES

[1] EU-U.S. Trade Talks: European Commission presents draft negotiating mandates. http://europa.eu/rapid/press-release_IP-19-502_en.htm

[2] F. Massacci, R. Ruprai, M. Collinson, J. Williams. Economic impacts of rules-versus risk-based cybersecurity regulations for critical infrastructure providers". IEEE Security & Privacy, 14(3), 52-60. 2015.

[3] F. D. Kramer and R. J. Butler, Cybersecurity: Changing the Model, 2019. https://www.atlanticcouncil.org/images/publications/Cybersecurity-Changing_the_Model.pdf

[4] W. W. Powell, "Neither market nor hierarchy: Network Forms of organisation". Research in Organizational Behavior 12, pp. 295-336, 1990.

[5] V. Nevena, J. Freudiger, V. Bindschaedler, and J.-P. Hubaux. "The inconvenient truth about web certificates." In *Economics of information security and privacy iii*, pp. 79-117. Springer, 2013.

[6] J. Brito and T. Watkins. "Loving the cyber bomb-the dangers of threat inflation in cybersecurity policy." *Harv. National Security J.*, 3. 2011.

[7] L. Pupillo, "EU Cybersecurity and the Paradox of Progress," *CEPS Policy Insight*, 2018

[8] D. Hodson, Dermot and U. Puetter, "The European Union in disequilibrium: new intergovernmentalism, postfunctionalism and integration theory in the post-Maastricht period," *Journal of European Public Policy*, pp. 1-19, 2019

[9] M. Bevir, *Governance: A very short introduction*, OUP Oxford, 2012

[10] Regulation (EC) No 460/2004 of the Euro Parliament and of the Council of 10/March/2004 establishing the European Network and Information Security Agency, 2004 https://eur-

lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML

[11] EC. "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace". Joint communication to the European Parliament, the Council, the European economic and social committee and the committee of the regions, 2013. https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf

[12] EC. "The European Agenda on Security". Comm. to the European Parliament, the Council, the European economic and social committee and the committee of the regions, 2015.: http://www.europarl.europa.eu/cmsdata/125863/EU%20agenda%20on%20security.pdf

[13] EC. "EU cyber defence policy framework", 2018: http://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/en/pdf

[14] R A. Bendiek, Europe's Patchwork Approach to Cyber Defense Needs a Complete Overhaul, 2017. https://www.cfr.org/blog/europes-patchwork-approach-cyber-defense-needs-complete-overhaul

[15] A. Bendiek, R. Bossong, & M. Schulze, M., "The EU's revised cybersecurity strategy: half-hearted progress on far-reaching challenges", *Stiftung Wissenschaft und Politik Comment*, 47. Deutsches Inst. für Internat. Politik und Sicherheit. https://nbn-resolving.org/urn:nbn:de:0168-ssoar-55103-4

[16] EC. Draft report on the proposal for a regulation of the European Parliament and of the Council establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARL+PE-631.940+01+DOC+PDF+V0//EN&language=EN

[17] European Parliament legislative resolution of 17 April 2019 on the proposal for establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres. [online]: http://www.europarl.europa.eu/doceo/document/TA-8-2019-0419_EN.pdf

[18] R. Hoffman, N. Shadbolt, M. Burton, "Eliciting knowledge from experts: A methodological analysis." *Organizational Behavior and Human Decision Processes*, 129-158. 1995

[19] M.J. Spector, D.M. Merrill, J. Elen, J., M.J. Bishop, *Handbook of Research on Educational Communication and Technology*. New York, NY: Springer. 2014

[20] M. De Gramatica, F. Massacci, W. Shim, A. Tedeschi, J. Williams. "IT interdependence and the economic fairness of cybersecurity regulations for civil aviation." *IEEE Security & Privacy* 13, no. 5 52-61. 2015.

[21] M. de Gramatica, F. Massacci, F., W. Shim, U. Turhan, J. Williams, "Agency Problems and Airport Security: Quantitative and Qualitative Evidence on the Impact of Security Training." *Risk Analysis*, 37(2), 372-395. 2017.

[22] M. Halaweh, "Using grounded theory as a method for system requirements analysis." *Journal of Information Systems and Technology Management*, 23-38. 2012.

A STAKEHOLDERS TO BE INVOLVED

Participants were asked to select up to 8 among the following stakeholders groups:

- European Commission
- ENISA (European Network and Information Security Agency)
- National cyber security agencies
- Other national Government Representatives
- Industry
- Academia
- Industry associations
- Consumer associations
- Data Protection Authorities
- Computer Emergency Response Teams (CERTs, CSIRTs)
- Formal standards and/or certification organizations (e.g., ISO, ITU)
- Community standards and/or certification organizations (e.g., IETF)
- Community professional organizations (e.g., NANOG, community around RIRs like the RIPE NCC)
- Open Source software communities (e.g., the Linux foundation or the community around FOSDEM)
- Hacker communities (e.g., the German CCC or members of European Hackerspaces)
- Other

Pierantonia Sterlini (BSc International Studies, UTrento) has been the youngest president of the largest Italian Fair Trade Commercial Cooperative Organisation. She is now research project manager at UTrento. She is leading the education and capability work-package of the H2020 'CyberSecurity4Europe' pilot.

Fabio Massacci (PhD in Computer Engineering, URome La Sapienza). Has been at Cambridge, Siena and Toulouse and he is now full professor at UTrento. He published 250+ peer-reviewed papers and received the Ten Years Most Influential Paper award by the IEEE RE'15 Conference for his work on security requirements. He coordinated several EU project including the project SECONOMICS "Socio-economics meet security". He participates to the CVSS SIG the world standard on vulnerabilities. He is member of the IEEE.

Natalia Kadenko (PhD in Political problems of International Systems and Global Governance, TS National University of Kyiv) used to work as an editor and political analyst, as well as cooperated with an NGO specialized in peacekeeping research. She is currently a postdoc at TU Delft doing research in the field of cyber security governance.

Tobias Fiebig (PhD in Computer Networks, TU Berlin) worked as a Network engineer in industry and is now an Assistant Professor at TU Delft. He is currently involved in several national and international research projects, including the H2020 Safe-DEED project, and he is leading the Governance work-package of the H2020 'CyberSecurity4Europe' pilot.

Michel van Eeten (PhD TU Delft) is full professor at TU Delft and serves as the Director of the TPM Graduate School. He studies the interplay between technological design and economic incentives in Internet security. He has been leading a variety of research projects, funded by EU, NWO and industry, around the economics of cyber security and cybercrime. He serves on the Program Committee of the Workshop on Economics of Information Security. He is a member of the Dutch Cyber Security Council