UNIVERSITY OF TRENTO - Italy

TU Delft Delft University of Technology

Cyber Security for Europe

Governance Challenges for European CyberSecurity Policy: Stakeholders Views

First draft

P. Sterlini, F. Massacci

University of Trento, Italy

N. Kadenko, T. Fiebig, M. van Eeten

Technical University of Delft, The Netherlands

Governance Challenges for European CyberSecurity Policy: Stakeholders Views

EU H2020-SU-ICT-03-2018 Project No. 830929 CyberSec4Europe

Version I, May 2019

University of Trento
Department of Information Engineering and Computer Science
38123 Povo di Trento,
Via Sommarive 5 - Italy
Pierantonia Sterlini - p.sterlini@unitn.it
Fabio Massacci - fabio.massacci@unitn.it

The authors would like to thank Afonso Ferreira for jointly organizing a survey about the technological roadmap and the governance of the network and helping us to streamline it, Simone Fischer-Hübner and Pierre-Henri Cros for testing it and, above all, all interviewees who dedicated their time and effort to answer our questions.
This work has been supported by the EU H2020-SU-ICT-03-2018 Project No. 830929 CyberSec4Europe (cybersec4europe.eu). Authors contributions: scientifically supervised the re-search FM, MvE; designed research questions PS, FM, TF; collected data PS, FM; wrote the article NK, PS, FM.

Governance Challenges for European CyberSecurity Policy: Stakeholders Views

Pierantonia Sterlini, Fabio Massacci
University of Trento, Italy

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

Abstract— Existing and emerging cybersecurity threats require new models of multi-national and multi-stakeholder organizations to be tackled effectively. In this paper we outline possible approaches to cybersecurity governance and compare them against the recent cybersecurity policy initiative proposed by the European Union to establish a European Center and Network of Competence Centers which should be responsible to funnel all European cybersecurity funding in the next decade. Addressing a request from the European Commission, we test such policy proposal against the opinions of several key stakeholders (CISOs from Fortune 50 companies, senior administrators from European Agencies and Data Protection Authorities as well as managers from industry and academics). We illustrate some key policy issues that are broadly relevant across the Atlantic and the Pacific.

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

1 Introduction

THE last few years have seen a major emphasis on cyber security in the policy making area. It now spans technical issues affecting sensitive data of citizens or organizations with potential impact on elections, to the military defence against state actor. As an extreme witness of such changes, cybersecurity issues are now part of trade negotiations on pair with tariffs on automobiles. For example, negotiations are ongoing between the EU and the US through facilitated bilateral conformity assessment [1]. Policy makers faces several challenges to target their effort: should we propose more regulations and mandatory certifications? As government budgets are increasingly tight, should we prioritize technological research or broad professional skills development?

A key question in this respect is the type of governance that should be in charge of such policy initiatives. The diverse, evolving, and global nature of the cyber threats requires responses stemming from coordinated partnerships, which may be executed through the framework of competence centres.

For example, the Atlantic Council report on cybersecurity [2] recommends introducing a "state-centric cybersecurity expert centre" in the US as a part of new cybersecurity governance model; furthermore, the report mentions "organizing around like-minded countries", i.e., intensifying international cooperation with strategic partners and conducting joint campaigns in response to cyber threats.

In a similar fashion, the European Commission has proposed a legislation introducing a competence centre and network of national centers that should be responsible for the European financing of technology, research and professional education for the upcoming decade.

Considering the wide diversity of stakeholders involved, ranging from government officials to hacktivists, the policy makers will be interested in how these groups see their role in the decision-making process, as well as their possible cooperation with existing entities.

In this paper we discuss several models for the governance of cybersecurity and how the recent legislative initiative of the European Union on a network of national should govern such policy issues. We report in this paper the preliminary opinions of several key stakeholders (CISOs from Fortune 50 companies, senior administrators from European Agencies and Data Protection Authorities as well as managers from industry and academics). Such findings can provide insight 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 [3] discusses three governance models: *market, hierarchy, and network*.

When it comes to cybersecurity governance, the invisible hand of the *market* is showing itself openly, if at times in a ham-fisted manner, world failures included [4]. Within this model, the economic exchange largely preserves the autonomy of the actors whose costs and benefits are self-assessed (for example, software cost vs cost of possible data loss), and no long-term feeling of trust and obligation emerges. Where consistent overarching governing approach of national and EU bodies is often lacking, market mechanisms step in to address immediate issues. We can observe market-based stakeholders taking the lead by focusing on technological solutions, since cyber threats have the potential to undermine their profits. The necessity of adding non-market-driven complimentary measures, however, is apparent for state security, or privacy for user data – which are as essential as the other aspects. In general, despite the prominent role of market leaders, the ever-evolving nature of cybersecurity threats

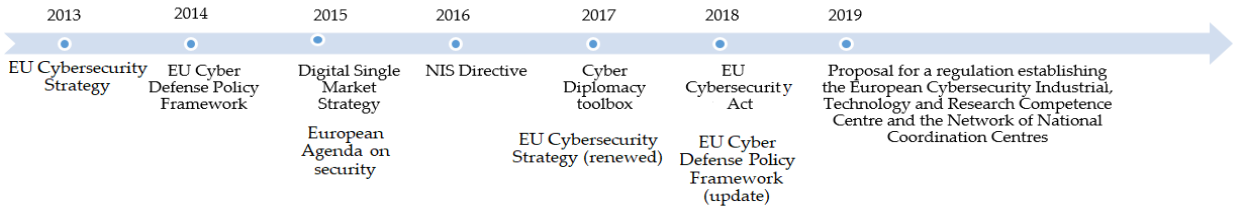

Fig. 1. The Recent European Policy Initiatives in CyberSecurity and the approval of the European Cybersecurity industrial, Technology and Research Competence Centre and the Network of National Coordination Centres.

has been often demonstrated the inefficiency of pure market-based governance and calls for a more diversified, multi-stakeholder approach.

The *hierarchical model*, with its rigid vertical, clear task distribution, and underlying skeleton of bureaucratic rules, according to Powell [3], is suited for high-speed mass production, compensating with stability and predictability for the uncertainty of market mechanisms. The backside of stability, however, is lack of flexibility that is necessary to react to the changes, let alone to anticipate them. Desire of predictability also generates tendencies toward compliance and 'box ticking' instead of proper risk analysis [5]. Unfortunately, for reacting to rapidly-shifting cybersecurity environment, high-speed flexibility is crucial. Hierarchical organizations also require a back-up of joint resource pool to safeguard for the inevitable insufficient responses. Yet, the request to pool additional resources by organizations in charge of security is always vulnerable to threat inflations by what US President Eisenhower called the military-industrial complex and for which piling 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.

One of the ways to realize an ambition for "cyber moonshot" is to act within the framework of what started out as an institutional moonshot of sorts – and namely, within the structures of the EU. A unifying goal of international cybersecurity cooperation answers the modern challenges of policymaking, 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 is best realized in the *network* governance model as described by Powell – "interdebtedness and reliance over the long haul" [3]. A feature of a successful network model is the facilitated 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 cybersecurity and resilience policy", elaborating on the inherent contradictory market incentives (private costs vs shared benefits). In other words, leaving cybersecurity to the domain of market-based relationships will likely fail to create the conditions necessary for efficient common policy responses, while hierarchical structure with the clear boundaries of specialization and authority may be inadequate for the challenge of uniting the cybersecurity research community by a common goal.

The network model is not immune to challenges, some of which are (perceived) loss of independence, unclear responsibilities, encapsulation. It is important to not disregard these challenges in designing the governance model that involves various European stakeholders. Like many other domains that require intense and timely cooperation, the network governance should avoid falling into the trap of enhancing its state of disequilibrium by producing short-term solutions and sacrificing the long-term stability for immediate political gains [8]. Collaborative governance, i.e., "attempts to bring all the relevant stakeholders together for face-to-face discussions during which policies are developed" [9] will help tackle the additional challenges, such as attracting talent and drafting the governance structure that would incorporate input from multiple stakeholders. The latter will ensure sustainable development of the governance model.

In short, good cybersecurity governance is supposed to answer to the following quality criteria:

- efficiency and capacity of resources allocation
- development potential and availability
- legitimacy and accountability
- transparency and sharing while allowing for data confidentiality.

The next section will look into the evolution of the diverse EU governance structures in the field of cybersecurity.

3 The EU CyberSecurity Policy Background

The history of the European cybersecurity 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 cybersecurity, 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 organisations in the European Union, thus contributing to the *smooth functioning of the internal market*" (our emphasis) [10]. The initial governance model was still the market model with information exchange as a key principle of successful governance.

3.1 The Recent Legislative Evolution

The change in international conditions has also lead to an evolution of the European Cybersecurity legislation which is illustrated in Figure 1.

The EU Cybersecurity Strategy from 2013 (updated in

2017), stressed the need for cooperation between Member States, private sector, and the EU agencies – ENISA (NIS), EC3/Europol (law enforcement) and EDA (defense) – to promote awareness of the cybersecurity threats, encourage investment, as well as to share best practices [11]. The 2015 European Agenda on Security focuses in combatting cybercrime as a key priority, which can be achieved through a "coordinated response at European level", including implementation of existing policies and adjusting the existing legislation [12]. The 2015 Digital Single Market Strategy demonstrates the awareness of the EU of the vital role of investments in novel technologies and support to SMEs. After a number of legislative pieces targeting specific cybercrime issues, such as payment frauds and electronic communication systems, The Directive on Security of Network and Information Systems across the EU (the NIS Directive) from 2016 is an example of general EU-wide legislative piece focusing on cybersecurity. It established the NIS group coordinating strategic cooperation among Member States, establishing 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 cybersecurity challenges [13]. In particular, attention is paid to conflict prevention and cooperation in cyber space, as well as to the availability of information; the updated priorities list includes development of cyber defense capabilities, training and exercises, research and technology, civil-military cooperation and international cooperation. The "cyber diplomacy toolbox" from 2017 provides framework for the joint foreign policy responses to cyberattacks against the EU, with the idea to "influence the behavior of potential aggressors in the long term". On the 11th of December, 2018, the European Parliament, the Council and the European Commission reached an agreement on the Cybersecurity Act, which, next to establishing an EU framework for cybersecurity certification, granted ENISA additional resources, thus reaffirming ENISA role in practical support of the Member states for cyberattacks management and prevention, as well as in the area of cyber-security policy-making. Whether ENISA was actually successful is debated as we shall see in the stakeholders interview Sections.

4 The Network of Competence Centers

Policy-makers often find it a challenge to write about European governance and EU policies without mentioning the word "crisis", or, more kindly, "patchwork approach"[14] and "half-hearted progress"[15]. With the growing body of the policy documents and legislative acts contributing to cybersecurity governance, several challenges became apparent. First, the EU-wide issue of maintaining balance between national freedoms and supranational regulations remains problematic. For cyber threats the distinctions between these domains become even less clear. From identification of the attacker to developing the most efficient responses, the area increasingly requires intra- and international cooperation, as well as cross-domain policy responses (justice, international security and harmonization of education are some examples). Additionally, as outlined in the previous section, market players are an important player in the field. The emerging multi-national, multi-stakeholder cybersecurity network model, while correctly identifying the existing challenges and aiming for transparency, accountability, sufficient development potential and resources allocation, suffers from the issues of efficiency, overlapping competencies, and independence. The governance process is further complicated by the nature of the inter-institutional cooperation between the EU bodies.

Within this background, the need for a better coordination of the EU funding of cybersecurity 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 defence: Building strong cybersecurity for the EU", which proposed establishing an EU cybersecurity competence centre with a network of national coordination centres.

On 7 December 2018 a rapporteur from the European parliament presented the draft report, which welcomed the Commission's initiative and, while stressing the coordinating role of ENISA in the Competence Centre's activities, explicitly called for a role by experts, large and small companies. The report endorsed a multi-stakeholder approach and the vision of cybersecurity as a flexible, involving field that requires a more creative approach than a series of products. [16]

At the time of writing, a proposed amendment by the European Parliament [17] fits within the idea of collaborative governance by explicitly defining stakeholders as

> "*industry, public entities and other entities which deal with operational and technical matters in the area of cybersecurity, 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:

> "*…should deliver cybersecurity-related financial support from the Horizon Europe and Digital Europe programmes, as well as from the European Defence Fund for actions and administrative costs related to defence, and should be open to the European Regional Development Fund and other programmes where appropriate. This approach should contribute to creating synergies and coordinating financial support related to Union initiatives in the field of cybersecurity 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

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

Four pilot projects were launched in 2019, aimed to "assist the EU in defining, testing and establishing the governance model of a European Cybersecurity Competence Network of cybersecurity centres of excellence"

The stakeholders survey that we discuss in the next section was performed in the framework of one of those pi-

lots (CyberSec4Europe) with the explicit task of collecting the opinion of a variety of stakeholders on the possible governance of the Network.

5 Collecting Stakeholders Viewpoints

Various techniques exist for knowledge elicitation [18] but a variant of structured or semi-structured interviews are most commonly involved in task analysis (See Chap 42 in [19]). To collect the opinion of stakeholders we took a two pronged approach as previously done in [20][21]for cyber-security policy analysis of stakeholders.

On one side a structured survey with over 50 stakeholders in order to collect suggestions and opinions about the governance model for the Competence Network on the other a focused personal interviews based on the notion of "grand tour interviews" [22]. The survey included both a number of open answers as well as multiple choices answers to provide a summary quantitative analysis of the results. The actual questions presented to the stakeholders are given in the appendix. The expected time to complete the 24 either open-ended or closed-ended 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 April 2019 and made available to the industrial and academic members of the pilots (with an audience of around 200 potential respondents). The total number of completed answers by April 30th, 2019 was 42.

At the time of writing, the European CyberSecurity Organization agreed to circulate the survey to its members and therefore a much wider circulation is expected.

TABLE 1
DEMOGRAPHICS FROM THE STAKEHOLDERS SURVEY

Academy	*Industry*	*Nat. Regulator/Agency*	*Research/Trade Association*
20	17	3	2

The participants came from 16 Members States of the European Union. Three of them did not specify their nationality.

VERTICAL INDUSTRY DOMAINS OF PARTICIPANTS

Health	*Finance.*	*Incident Reporting*	*Supply Chain*	*Smart Cities*	*Identity Mngt*
2	3	3	5	6	9

Multiple answers are possible. 16 (academic) participants did not identified 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).

5.1 Key Findings

When asked about what Europe should achieve as an *overall goal* in cybersecurity, *coordination* was identified as the most important goals together with independence from non-EU countries with regards to technology and protection of citizens, businesses and state actors.

In terms of *what should change to improve* the situation (e.g. better resilience, transparency, trustworthiness, security metrics...) respondents considered transparency of decision-making trustworthiness and resilience as challenges. The Standardisation of certification of infrastructures, service, and products were also indicated as aspects that should change in the European cybersecurity scenario.

When asked "In your area, what *key capabilities* are required by systems, people, institutions, etc., to achieve that change?" participants agreed that education at all levels is one of the most important aspect for raising cybersecurity and privacy awareness. **In particular, most highlighted that cybersecurity needs a networking of professionals, or better a *new generation of experts of cybersecurity trained through an interdisciplinary approach* (who master both the security of systems but also understand how cybersecurity affects the business**).

Since the Network is supposed to decide *where cybersecurity funding should go* **a key question is whether it should focus on technology or on other measures**. **In this respect there seems to be no clear cut consensus among the participants.** Indeed, only 31% (13 out of 42) of the participants to the survey consider the developments of better security technologies as essential and (14 out of 42) consider it of major importance. Around 40% of the participants (17 out of 42) consider the new or improved technical standards of major importance.

In terms of non-technical measures half of the respondents (21 replies) consider new professional or academic skills as essential to achieve the capabilities. Approximately half of the participants (20 out of 42) consider policy interventions of major importance. New certification and audit procedures are of major importance for 14 participants out of 42.

Another extremely hot policy questions is whether the *Network should push different national centres (and the industries gravitating around them) towards specialization*. This is also an extremely relevant question of the US or other countries that have pushed for a model of distributed network centres. When asked only a third (15 participants) replied supported the option of pushing towards specialization. A similar number, 31% (13 participants) considered it is possible only in special cases, and 28% (12 participants) express a negative opinion.

Another interesting policy question is whether the *Network should push towards mandatory security certification at European level*. This question has a major policy implication. Indeed, in the initial text of the Commission there was a provision for identifying areas where security certification was to be mandatory. A strong lobbying effort from industry has significantly weakened the wording: at the time of writing only voluntary certification schemes are considered in the legislative texts under consideration. In this respect the majority of participants (23 out of 42) agreed that the Network and Centre should push towards mandatory security certification at European level.

With regard to the *key players*, participants were asked to indicate at most 8 players out of a broad list of players to choose from (listed in Appendix B).

The majority of the participants (27 out of 42) consider the European Commission as a key player. 26 partici-

pants indicated ENISA. What emerged a as a surprise what the strong role that all parties attributed to *Data Protection Authorities (24 out of 42)* almost at the same level as the European Commission thus showing the key important that privacy protection has for European citizens. Another important role was assigned by participants to Computer Emergency Response Teams (CERTs, CSIRTs) – 15 out of 42--, which is comparable to the role assigned to academia. This finding calls into question the view point of some decision makers who see the role of the network as mostly a vehicle to fund research and innovation activities. We specifically asked participants about their opinion on ENISA. Of those respondents who expressed an opinion, most regarded ENISA as a potential coordinator, with an "orchestration role".

4 High Profile Interviews

To provide a higher level of insight we have identified a number of key players. In this section we report on the preliminary finding for the first 10 key high profile interview (additional 20 are currently under analysis).

Through a purposive sampling approach [22] we identified some stakeholders to represent a variety of roles specifically involved in the cybersecurity field (from agency representatives to data protection authorities, from CISOs to representatives of customers organizations. For 10 stakeholders who agreed to be formally interviewed in persons, we conducted in-depth semi-structured interviews which were recorded with participants' permission and transcribed into anonymous form. They are listed in Table 2 and were all interviewed in March-April 2019.

We illustrate these finding by the considerations of some stakeholders representative of the different roles in the area as they help to clarify the findings behind the survey. **Starting from the *key goal of the network*, most users agreed that one of its objectives was to distribute research funding and support technological innovation [#1, #2, #3, #7, #10] but they widely diverged on whether this was the main if not only task (as suggested by [#2]). For example, three very diverse stakeholders [#3, #6, #10] raised the critical importance, shared also by the European Parliament, of supporting SMEs to bring research to the market, while others [#1, #4, #8, #9] focused on the importance of professional skills and education.** A key policy issue in terms of international relations and the current discussion on trade and protectionist issue in the US was also raised by some stakeholders [#1, #3]: how to make sure that the European taxpayer money invested in cybesecurity research through open calls does not benefit US companies through their EU subsidiaries. Professional knowledge and skills returned also among the *key capabilities* to be achieved. Some stakeholders [#4, #7, #9] highlighted to the constant need for knowledge to be updated to address the dynamic changes in cybersecurity and several others highlighted the key role that the Network could have in terms of sharing of data in particular sharing attack data in a way that would protect the identification of the victim while allowing other actors to protect themselves [#1, #4, #8, #9].

TABLE 2
DEMOGRAPHICS OF HIGH PROFILE INTERVIEWS

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 Multinat. Co.
8	Vice President	Re-Insurance Multinational Co.
9	President	Critical Infrastructure Org.
10	CISO	Big Pharma and Energy Multinational Co.s

Interviewees company or role anonymized to avoid re-identification.

An interesting issue raised by some stakeholders (e.g. [#1, #4, #5, #9]) was how normal citizens or ethical hackers could turn to start notifying security issues and whether the corresponding regulator of each vertical domain could be a potential first point of contact as the company which has the security issues would have clearly a conflict of interest. The general issue of responsible disclosures is indeed still unsolved.

Another important policy question was whether EU should use the *Network to specialize the research by each national center* (i.e. target funding on one particular research area in one member state wrt another). The (strong) feeling of potential duplication of effort was mostly felt by stakeholders with a European responsibility (e.g. [#2, #3]) who explicitly mentioned wasted resources by duplication). However this view was not shared by other stakeholders and even potentially backfiring. For example [#4, #6, #10] 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. The question on who should be the *key players* produced a variety of responses but most interviewees argued that such decision should be left at Member State levels. As [#3, #4, #5] observed, different Member States would have different sensibilities and eventually also different agencies in charge of national security (e.g. BSI in Germany, ANSSI in France and the DIS in Italy, each referring to a different type of Ministry). Indeed, it was noted [#3, #4, #9] that eventually cybersecurity will always have a key role for national security and such role is not eliminable by purely considering market issues.

Also in this case a role by ENISA was not supported by several stakeholders. Some [#3, #10] noted that anything significantly effective have not and would not come out due to the lack of resources.

5 CONCLUSIONS

There seems to be a general consensus that the flexibility of the network model seems the most appropriate to cope with the dynamic challenges of cybersecurity and to provide the flexibility to adapt to the different states economic and policy conditions. Such flexibility also implies that there should be no centralized decision on the actual form that is used for the individual national centers.

In terms operational and decision making rules another broad consensus exist on the issue of promoting information sharing about security issues and possibly coming to unifying technical standards about cybersecurity. The significant agreement on the presence of CERTs among the stakeholders (before academics and second only to the quite obvious European Commission and ENISA) shows the clear importance in this phase of the issue of incident management.

Yet, there is no convergence on the relative importance of technological development vs professional skill development. A safe conclusion should likely be that both should be supported.

REFERENCES

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

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

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

[4] 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, New York, NY, 2013.

[5] 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.

[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, post functionalism 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, [online]: 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. [Online]: 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. [Online]: http://www.europarl.europa.eu/cmsdata/125863/EU%20agenda%20on%20security.pdf

[13] EC. "EU cyber defense policy framework", 2018. [Online]: 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 [online] 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 Institute für Internationale Politik und Sicherheit. [online] 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 Centers [online] 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.

Cyber Security for Europe

—

Contact info:
Pierantonia Sterlini - University of Trento
p.sterlini@unitn.it