Governance Challenges for European CyberSecurity Policies

Stakeholder Views

Sterlini, Pierantonia; Massacci, Fabio; Kadenko, Natalia; Fiebig, Tobias; van Eeten, Michel

DOI
10.1109/MSEC.2019.2945309

Publication date
2019

Document Version
Final published version

Published in
IEEE Security and Privacy

Citation (APA)
Sterlini, P., Massacci, F., Kadenko, N., Fiebig, T., & van Eeten, M. (2019). Governance Challenges for European CyberSecurity Policies: Stakeholder Views. *IEEE Security and Privacy*, *18*(1), 46-54. Article 8887440. https://doi.org/10.1109/MSEC.2019.2945309

Governance Challenges for European Cybersecurity Policies: Stakeholder Views

Pierantonia Sterlini and Fabio Massacci | University of Trento
Natalia Kadenko, Tobias Fiebig, and Michel van Eeten | Technical University of Delft

We outline possible approaches to cybersecurity governance and compare them against the proposed European Union network of competence centers. We survey stakeholders for their opinions about the centers and analyze the results.

Security issues affect the private data of millions of citizens. Organizations that influence elections and state actors that attack critical infrastructures have made cybersecurity a focus of policy makers. Cybersecurity governance and conformity are now part of trade negotiations alongside traditional issues, such as tariffs on cars, between the European Union (EU) and the United States.[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.[2] The diverse, distributed, evolving, and global nature of cyberthreats often requires responses that stem from coordinated partnerships. Therefore, when deciding whether to prioritize research or skills development, policy makers need a ground truth about the needs of existing stakeholders to avoid impractical frameworks that may hinder existing collaborations.

For example, an Atlantic Council report[3] recommends a "state-centric cybersecurity expert center" in the United States as part of a new governance model. It also mentions "organizing around like-minded countries"; that is, intensifying international cooperation and conducting joint campaigns in response to cyberthreats. Similarly, the European Commission has proposed a cybersecurity competence center and network of national centers that would oversee cybersecurity R&D financing in the EU. The legislative process has broadened its scope; for example, to include professional education. The cybersecurity competence center is an interesting case study for cybersecurity governance, given the wide diversity of the stakeholders, from government officials to hacktivists. We are interested in understanding how those groups see their role and what they think the final goal of the cybersecurity competence center should be.

Digital Object Identifier 10.1109/MSEC.2019.2945309
Date of current version: 30 October 2019

The core of our contribution is the analysis and empirical validation of different models of cybersecurity governance for the cybersecurity competence center to inform the European Commission and European Parliament decision-making process. We seek to examine three research questions (RQs) drawn from theory, legislative proposals, and the direct opinions of European stakeholders to see whether they are aligned:

- *RQ 1 (narrow or broad focus)*: Do stakeholders envision a focus on R&D or broader goals (for example, professional skills and transfers to market)?
- *RQ 2: (decision making)*: What governance framework structure do the stakeholders think will achieve their target cybersecurity capabilities?
- *RQ 3 (key players)*: Which organizations do the stakeholders want to leverage and rely on for an EU-wide cybersecurity competence network?

To answer those questions, we first discuss several models of governance and how the EU cybersecurity competence center initiative fits them. We then conduct a quantitative and qualitative study of EU stakeholders (chief information security officers from Fortune 50 companies, senior officers from EU agencies and data-protection authorities, industry managers, hacktivists, and academics) to collect their opinions. Our findings shed light on the key issues that policy makers should address when designing a governance model for cybersecurity.

Governing Cybersecurity?

There is no one-size-fits-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 shows itself openly, including its failures around the world.[5] The economic exchange largely preserves the autonomy of actors whose costs and benefits are self-assessed (for example, software costs versus the expense of possible data loss), and no long-term feeling of trust and obligation emerges. When there is an insufficient governing approach at the national level, market mechanisms address immediate needs. We can expect market-based stakeholders to ask the cybersecurity competence center for R&D solutions, since cyberthreats have the potential to undermine their profits (the narrow focus in RQ 1). Stakeholders that favor the market model would likely prefer a decision-making process that granted limited powers to the EU body (RQ 2). Industry players would probably be named as key stakeholders (RQ 3).

With its rigid, vertical, and clear task distribution and bureaucratic rules, the hierarchical model is suited to high-speed mass production, replacing the uncertainty of market mechanisms with stability and predictability, according to Powell.[4] The downside of stability is a lack of flexibility to anticipate and react to changes. The desire for predictability may nudge actors toward compliance and "box ticking" instead of proper risk analysis.[2] Unfortunately, flexibility may be crucial to quickly reacting to the rapidly shifting cybersecurity environment. Hierarchical organizations also require a backup joint resource pool to safeguard against inevitable insufficient responses.

Yet, requests for additional resources from cybersecurity "defenders" are always vulnerable to threat inflations by what U.S. President Dwight Eisenhower called the military-industrial complex and for which robust evidence exists in the cyber domain.[6] This model's most difficult challenge is that it 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. The model includes space for broader goals that could be reflected by stakeholders expressing their desire for a wider focus (RQ 1). The European Commission would likely be named the primary decision-making power (RQ 2). Stakeholders may also require the involvement of multiple parties rather than allowing industry to settle the rules of the game (RQ 3).

An alternative to realizing a "cybermoonshot" is to consider the cooperative framework of what started out as an institutional moonshot of sorts; namely, the EU. A model of international cybersecurity cooperation may answer the challenges of cybersecurity policy making, similar to the way that the EU prototypes were the answer to the challenges of peace building in postwar Europe. A common European goal may be best realized in the network governance model, which includes, as described by Powell, "interdebtedness and reliance over the long haul."[3] 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 states that "trust-based relationships are essential to cybersecurity and resilience policy" and elaborates on the inherent contradictory market incentives (private costs versus shared benefits). In other words, leaving cybersecurity 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 challenges of a dynamic environment.

Stakeholder answers that indicated a preference for the network model would include the need to tackle broad, ambitious cybersecurity goals (RQ 1) by opting for a decision-making process based on consensus and involving multiple parties (RQs 2 and 3). The network

model is not immune to challenges, such as a perceived loss of independence, unclear responsibilities, and encapsulation. Like many domains that require intense and timely cooperation, it must avoid falling into a state of disequilibrium as a result of producing short-term solutions and sacrificing long-term stability for immediate political gains.[8] Collaborative governance, that is, "attempts to bring all relevant stakeholders together for face-to-face discussions during which policies are developed,"[9] will help to tackle additional challenges, such as attracting talent, incorporating relevant input from diverse stakeholders, and ensuring sustainable development.

EU Cybersecurity Policy

How has the real-life cybersecurity competence center legislative process responded to the governance challenges? Policy makers often find it challenging to write about EU rules without mentioning a "patchwork approach"[14] and "half-hearted progress."[15] With the growing body of policy documents and legislative acts covering cybersecurity, several challenges have become apparent. The EU-wide issue of maintaining a balance between national freedoms and supranational regulations remains problematic because for cyberthreats the distinction between those areas is unclear. From identifying attackers to developing the most efficient responses, cybersecurity increasingly requires intra- and international cooperation as well as cross-domain policy responses (for example, justice, international security, and the harmonization of education). Additionally, international market forces are an important player in the field.

The Legislative Evolution

The history of the European cybersecurity network begins with the adoption of the Budapest Convention on Cybercrime in 2001, the Common Framework on Electronic Communications Networks and Services in 2002, and the establishment of the European Union Agency for Cybersecurity (ENISA) in 2004. The main tasks for 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."[10] The model was based on the market, with information exchange as a principle of successful governance.

Changes in international conditions led to the evolution of EU cybersecurity legislation (Figure 1). The EU Cybersecurity Strategy from 2013 (updated in 2017) stressed the need for cooperation between member states, the private sector, and EU agencies (ENISA, the European Crime Center/Europol, and the European Defense Agency) to promote awareness of threats, encourage investment, and share best practices.[11] The 2015 European Agenda on Security focused on combatting cybercrime through a "coordinated response at the European level," including implementing 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 small- and medium-sized enterprises (SMEs). After several pieces of legislation targeting specific cybercrime issues (for example, payment fraud), the Directive on the Security of network and information systems (NISs) was issued in 2016 and provided an example of an EU-wide initiative. It established an NIS group to coordinate strategic cooperation among member states, provide guidelines for national capabilities, and promote the exchange of information.

The EU Cyberdefense Policy Framework, adopted in 2014, was updated in 2018 to better correspond to new challenges.[13] Attention was paid to conflict prevention and cooperation in cyberspace as well as the availability of information. The updated priorities list included the development of cyberdefense capabilities, training, and exercises; research and technology; and civil-military and international cooperation. The "cyberdiplomacy toolbox" from 2017 provided a framework for joint foreign-policy responses to cyberattacks against the EU to "influence the behavior of potential aggressors in the long term."

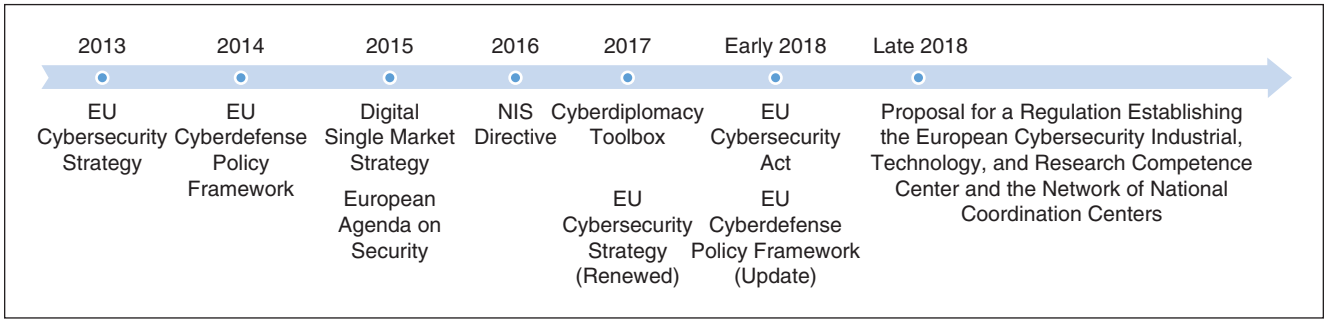

Figure 1. The evolution of the European cybersecurity policy initiatives.

In December 2018, the European Parliament, European Council, and European Commission reached an agreement on the Cybersecurity Act, which established an EU framework for cybersecurity certification and granted ENISA additional resources, thus reaffirming the agency's role of supporting member states in cyberattack management and prevention as well as in cybersecurity policy making. Whether ENISA was actually successful in fulfilling that function is debated, as we shall see in the stakeholders' interviews.

The evolution showed that Europe's goals were broadening (RQ 1) from narrow and market based to an accommodation of intense cooperation at different levels (RQ 2) with diverse stakeholders involved (RQ 3) in the network model. The political debate also raised the need for stronger cybersecurity governance at the EU level and better coordination at the operational scale, including the mitigation of organizational fragmentation and better resource utilization.

The Network of Competence Centers

Against that background, it became apparent that EU cybersecurity funding needed to be better coordinated, as identified by the last steps in Figure 1. On 13 September 2017, the European Commission issued a communication, "Resilience, Deterrence, and Defense: Building Strong Cybersecurity for the EU," which proposed establishing the cybersecurity competence center with a network of national coordination hubs. The European Commission's initial intent was that the cybersecurity competence center would coordinate research funding (RQ 1). In December 2018, a rapporteur from the European Parliament presented a draft report that stressed the coordinating role of ENISA in the cybersecurity competence center's activities and called for an advisory role for experts and large and small companies (the hierarchical model, RQ 2). The report endorsed a multistakeholder approach and the vision of cybersecurity as a dynamic field that required a more creative approach than a series of products.[16]

At the time of writing, the "Proposal for a Regulation Establishing the European Cybersecurity Industrial, Technology, and Research Competence Center and the Network of National Coordination Centers" passed the European Parliament. One proposed amendment[17] fit the idea of collaborative governance (the network model, RQ 2) 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, interalia trade unions, consumer associations, the free and open source software community, and the academic and research communities."

Another amendment addressed capacity (RQ 1), saying that it "should deliver cybersecurity-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 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 that "the Union needs to be able to adapt fast and continuously to new developments in the field. Hence, the [cybersecurity competence center] 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 resource allocation, may suffer from inefficiency, overlapping competencies, and conflicts of independence. The governance process is further complicated by the nature of the interinstitutional cooperation between EU bodies. Four pilot projects were launched in 2019 to "assist the EU in defining, testing, and establishing the governance model" of the cybersecurity competence center. Our research was performed in one of them, CyberSec4Europe.

Collecting Stakeholder Viewpoints

Various techniques exist for knowledge elicitation,[18] but a variant of structured and semi-structured interviews is the most commonly used (see chapter 42 in Spector et al.[19]). To collect the opinions of stakeholders, we took a two-pronged approach, as previously done by De Gramatica et al[20] and Halaweh,[21] to stakeholder cybersecurity policy analysis. A structured survey was given to more than 50 stakeholders to collect suggestions and opinions about the governance model, and it was supplemented by 18 face-to-face discussions based on the notion of "grand tour interviews."[22]

The Survey

The survey included open and multiple-choice questions to provide a quantitative analysis of the results. The expected time to complete the 24 questions was 15–20 min. The demographics of the stakeholders who responded are summarized in Table 1. The survey was open from mid-March through the end of August 2019 and made available to the industrial and academic members of the cybersecurity competence center pilot programs (which yielded roughly 200 potential respondents). Fifty-seven completed surveys were collected. At the time of writing, the European Cybersecurity

Table 1. The demographics of the survey participants.

Work sector			
Academy	Industry	Regulator, agency	Trade association
26	25	Three	Three

The participants came from 16 member states of the EU. Five were from outside the EU, and two did not specify their nationality.

Table 2. The vertical domains of the industry participants.

Health	Finance	Incident reporting	Supply chain	Smart cities	Identity management
Five	Three	Four	Six	Six	Nine

Multiple answers were permitted. Eight participants did not identify a domain. The vertical domains closely mirror those of the European Cybersecurity Organization.

Table 3. The stakeholders' professions.

Number	Role	Organization
1	Senior manager	European Union Agency for Cybersecurity
2	Board member	European Union Agency for Cybersecurity
3	Board member	European trade organization
4	Board member	EU data-protection supervisor
5	Senior manager	European consumer organization
6	Ethical hacker	Self-employed
7	Senior manager	Semiconductor multinational corporation
8	Vice president	Re-insurance multinational corporation
9	President	Critical-infrastructure association
10	Chief information security officer	Pharmaceuticals and energy multinational corporations
11	Professor	University
12	Policy advisor	Cybersecurity for industry and government
13	Government official	National government, IT security
14	Professor, entrepreneur	University, small security company
15	Ethical hacker	Security industry
16	Professor	University
17	Vice president	Software multinational corporation
18	Senior manager	Financial institution

Organization agreed to circulate the survey to its members for a major consultation event to take place in November 2019.

The Interviews

Through a purposive sampling approach,[22] we identified stakeholders (Table 2) to represent a variety of roles that were specifically involved in cybersecurity (from agency representatives to data-protection authorities and chief information security officers to representatives of customer organizations). For the 18 additional stakeholders (Table 3) who agreed to sit down with us, we conducted semistructured interviews that were recorded with the participants' permission and transcribed anonymously. All of the interviews were conducted between March and June. They enabled us to supplement and clarify the survey's findings.

The Questions

The survey and interviews featured questions that were designed to elicit answers in a terminology close to the stakeholders' own interests. For example, a stakeholder that did not participate in the cybersecurity competence center pilots was unlikely to be interested in generic questions on governance. However, that person would have opinions about the capabilities that Europe should develop and who should be in charge of achieving them (for example, using the hierarchy and market models).

Our questions began with the overall cybersecurity goals that Europe should achieve (such as the coordination of policies, technological independence, and protection of citizens and state actors from non-EU countries). For example, technological independence is a central EU policy priority given the current U.S. protectionist measures (such as its restrictions on Huawei). To achieve that goal, we also asked what should change. Then we asked, "In your area, what key capabilities are required by systems, people, institutions, and so forth 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, the participants were asked to select at most eight stakeholder groups from a broad list (see "Identifying the Stakeholders"). We then focused on the decision-making aspects of the cybersecurity competence center. Another significant question was whether the network should push the national centers and the industries flocking around them toward specialization (that is, fund a research area in one member state only, as the "avoiding duplication" clause in the legislation is often interpreted to mean). This is an important question for the United States[3] and other countries that opt for distributed network centers (for example, the United Kingdom).

In terms of mandates, we asked whether the center and its network should advocate compulsory security certification at the European level. In the initial European Commission text, there was a provision for identifying areas that would be subject to mandatory security certification. Industry lobbying efforts have weakened the wording, and at the time of writing, only voluntary certification schemes are considered in the legislative documents.

Analysis

In terms of what should change to improve the cybersecurity situation (for example, better resilience, transparency, trustworthiness, security metrics, and so forth), respondents considered the transparency of cybersecurity decisions, trustworthiness, and resilience to be challenges. Some interviewees (interviewees 4, 7, 9, and 17) highlighted the need for knowledge and education to be constantly updated to meet the dynamic changes in cybersecurity. There must be new generation of experts trained through an interdisciplinary approach to master system security and understand how cybersecurity affects business. Some participants raised the issue of making sure that EU taxpayer money to fund cybersecurity research does not benefit U.S. companies through their European subsidiaries (interviewees 1 and 3). In general, the goal was to achieve cybersovereignty, independence, and control (interviewees 1, 3, 11, and 14–16), with a clear preference for a broader focus (RQ1) and indications of support for the hierarchical and network models.

Our survey results indicated that activities should go beyond funding R&D and include training and innovation. Only 32% of the participants considered the development of better security technologies to be essential, while 35% believed that it was of major importance. Less than half (42%) considered new and improved technical standards to be essential. In contrast, 46% of the respondents replied that new professional and academic skills were critical to achieve cybersecurity capabilities. Slightly more than half (51%) believed that policy interventions held major significance.

The interviewees agreed that R&D funding was an important objective (interviewees 1–3, 7, and 10), but they widely diverged on whether it was the only one (as advocated by an EU actor, stakeholder number 2). For example, three very diverse stakeholders (interviewees 3, 6, and 10) raised the critical need to support SMEs to bring research to the market, a view shared by the European Parliament. Others (interviewees 1, 4, 8, 9, and 17) focused on professional skills and education. Since all three models are consistent with those opinions, we must look to other answers to see how the goals should be met. The certification of infrastructures, services, and products were also shown to be aspects that should change (it was of major importance to one third of the respondents). In that respect, half of the participants agreed that the cybersecurity competence center should support mandatory security certification. Such answers lean toward hierarchical models.

Identifying the Stakeholders

Participants were asked to select up to eight of the following stakeholder groups:

- European Commission
- European Network and Information Security Agency
- National cybersecurity agencies
- Other national government representatives
- Industry
- Academia
- Industry associations
- Consumer associations
- Data-protection authorities
- Computer emergency response teams
- Formal standards and/or certification organizations (e.g., the International Organization for Standardization and International Telecommunications Union)
- Community standards and/or certification organizations (e.g., the Internet Engineering Task Force)
- Community professional organizations (e.g., the North American Network Operators' Group and bodies related to the Regional Internet Registries, such as the Réseaux IP Européens Network Coordination Centre)
- Open source software communities (e.g., the Linux Foundation and the Free and Open Source Software Developers' European Meeting)
- Hacker communities (e.g., the German Chaos Computer Club European Hackerspaces)
- Other.

The quest to specialize research in each national center was not supported by the stakeholders. Less than one third of the respondents (28%) supported the option, one quarter considered it to be possible only in special cases, and the remainder expressed a negative opinion. Concerns about potential duplication were held mostly by stakeholders who had a Europe-wide responsibility (for example, interviewees 2 and 3, who explicitly mentioned wasted resources). Other stakeholders who believed that the scheme might backfire did not share the view. For example, interviewees 4, 6, 10, and 17 believed that the policy would be effective only during the short term, since it is not possible to predict where new innovations will take place. Others (interviewees 4, 10–13, and 16) stated that specialization will occur naturally and should be capitalized rather than enforced. Those answers strongly support the network and market models over the hierarchy model.

A majority of the participants (60%) considered the European Commission and ENISA (61%) to be important players. However, nearly one fifth (18%) indicated only the European Commission. Vice versa, a similar number of respondents (19%) pointed to ENISA without mentioning the European Commission. That can be interpreted as a preference for clear task distribution through a designated structure, which corresponds to the hierarchical model. Still, many stakeholders were not familiar with ENISA. Of those respondents who expressed an opinion, most assigned ENISA to an orchestration role, underlining the need for harmonization between organizations (as stated by number 17). Some interviewees (interviewees 3 and 10) noted that ENISA has done nothing effective and probably will not, due to a lack of resources.

Most of the interviewees argued that decisions should be left to the member states and that a balance between different stakeholders was desirable. As interviewees 3–5 observed, different member states would have varying sensibilities and agencies in charge of national security (for example, the Federal Office for Information Security in Germany, National Cybersecurity Agency of France, and Department of Information Security in Italy). Cybersecurity will always have a critical role in national security that cannot be eliminated by market issues (as stated by interviewees 3, 4, and 9). Such answers, again, strongly support the network model.

What emerged as a surprise was the role of the cybersecurity competence center as a first point of contact to support society (from SMEs to individual citizens) when it needs cybersecurity advice. A majority of the participants (68%) assigned academia a fundamental cybersecurity role, which is expected for centers that receive research funding. Nearly half of them said the computer emergency response teams (CERTs) should have an advisory role. Several interviewees (interviewees 1, 4, 8, and 9) believed the cybersecurity competence center could promote mechanisms for sharing attack data that protected victims' identities and enabled other actors to shield themselves. Others (interviewees 1, 4, 5, and 9) believed that citizens and ethical hackers could report security issues to the cybersecurity competence center to pass on to the appropriate regulator, since the companies that were involved would have a conflict of interest. In addition, 58% of the respondents attributed an important role to the data-protection authorities, which was comparable to the number of participants who selected the European Commission, thus demonstrating the importance that privacy protection has for European citizens.

Ambiguous views of the cybersecurity competence center emerged from the survey. The stakeholders projected their concerns, interests, and ambitions for European cybersecurity onto the agency. To some extent, that simply reflects the diversity of the parties operating in this area. Even the European institutions have saddled their policies with diverse objectives, hopes, and requirements, a situation that emerged from a network approach rather than a hierarchical one.

The complex governance network that surrounds the cybersecurity competence center means that coordination and collaboration will not emerge purely from a shared vision or hierarchically determined structure. In the end, competing incentives will shape what the cybersecurity competence center will become and deliver. Those motives are the key for policy makers. What will the cybersecurity competence center and its funding structures reward? International collaboration? Research and development with industry? Products and technologies? Training and education? All of the above?

Concerning first RQ, there is no agreement on the relative importance of R&D versus skill development. Given the diverging viewpoints of our participants, we recommend allocating resources evenly in both directions. RQ 2 clearly elicited a preference for an informed network model (academics) with some elements of hierarchy (the European Commission and ENISA). The presence of CERTs among the stakeholders in charge of advising funding and education shows the importance of incident management in a cybersecurity governance framework, which is relevant to determining where the funding and educational skills should go (which plays only a minor role in today's education charters).

Concerning our third RQ, there seems to be a general consensus that the flexible network model is the best way to cope with cybersecurity challenges and

adapt to different economic and policy conditions. That flexibility implies that there should be no top-down decisions about the national centers' form and specialization, which has broad consequences for the Atlantic Council's proposal for the United States. In terms of operational and decision-making rules, another broad consensus exists on sharing security-issue information and possibly creating unified cybersecurity technical standards.

Eventually, if research funding remains the core of the network that will finally be approved by EU institutions, the broader ambitions for the cybersecurity competence center could be accommodated through incentives that reward linking research to societal impacts. An incentive embedded in funding schemes would strengthen the need for researchers to work with CERTs, industry partners, nongovernmental organizations, and so forth to improve security in the EU.

Acknowledgments

We thank A. Ferreira for jointly organizing a survey about the technological road map and the governance of the network, S. Fisher-Hubner and P.H. Cros for testing the survey, and all of interview subjects for their time. This work was partly funded by CyberSec4Europe within the European Union's Horizon 2020 program, H2020-SU-ICT-03-2018, under grant 830929. The opinions reported in this article are our own and not necessarily endorsed by the European Union or the survey respondents' organizations. ■

References

1. European Commission, "EU-U.S. trade talks: European Commission presents draft negotiating mandates," 2019. [Online].Available:http://europa.eu/rapid/press-release_IP-19-502_en.htm
2. F. Massacci, R. Ruprai, M. Collinson, and J. Williams, "Economic impacts of rules-versus risk-based cybersecurity regulations for critical infrastructure providers," *IEEE Security Privacy*, vol. 14, no. 3, pp. 52–60, May–June 2016. doi: 10.1109/MSP.2016.48.
3. F. D. Kramer and R. J. Butler. (2019). Cybersecurity: Changing the Model. Atlantic Council. Washington, DC. [Online]. Available: https://www.atlanticcouncil.org/in-depth-research-reports/report/cybersecurity-changing-the-model/
4. W. W. Powell, "Neither market nor hierarchy: Network forms of organization," *Res. Organ. Behav.*, vol. 12, pp. 295–336, Jan. 1990.
5. N. Vratonjic, J. Freudiger, V. Bindschaedler, and J.-P. Hubaux, "The inconvenient truth about web certificates," in *Economics of Information Security and Privacy III*, B. Schneier, Ed. New York: Springer-Verlag, 2013, pp. 79–117.
6. J. Brito and T. Watkins, "Loving the cyber bomb? The dangers of threat inflation in cybersecurity policy," *Harvard Law School National Security J.*, vol. 3, Apr. 2011.
7. L. Pupillo. (2018). EU cybersecurity and the paradox of progress. CEPS. Brussels, Belgium. [Online]. Available: https://www.ceps.eu/ceps-publications/eu-cybersecurity-and-paradox-progress/
8. D. Hodson and U. Puetter, "The European Union in disequilibrium: New intergovernmentalism, postfunctionalism and integration theory in the post-Maastricht period," *J. European Public Policy*, vol. 26, pp. 1153–1171, Jan. 2019. doi: 10.1080/13501763.2019.1569712.
9. M. Bevir, *Governance: A Very Short Introduction*. London: Oxford Univ. Press, 2012.
10. European Union, "Regulation (EC) No. 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency," 2004. [Online]. Available: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML
11. European Commission, "Cybersecurity strategy of the European Union: An open, safe and secure cyberspace," 2013. [Online]. Available: https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf
12. European Commission, "The European agenda on security," 2015. [Online]. Available: http://www.europarl.europa.eu/cmsdata/125863/EU%20agenda%20on%20security.pdf
13. Council of the European Union, "EU cyber defence policy framework," 2018. [Online]. Available: 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," Council on Foreign Relations, Aug. 30, 2017. [Online]. Available: https://www.cfr.org/blog/europes-patchwork-approach-cyber-defense-needs-complete-overhaul
15. A. Bendiek, R. Bossong, and M. Schulze, "The EU's revised cybersecurity strategy: Half-hearted progress on far-reaching challenges," German Institute for Security and International Affairs, Nov. 2017. [Online]. Available: https://nbn-resolving.org/urn:nbn:de:0168-ssoar-55103-4
16. Committee on Industry, Research, and Energy, "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," European Parliament, Brussels, Belgium, Rep. 2018/0328(COD), 2018. [Online]. Available: 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, "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," 2019. [Online]. Available: http://www.europarl.europa.eu/doceo/document/TA-8-2019-0419_EN.pdf

18. R. Hoffman, N. Shadbolt, M. Burton, and G. Klein, "Eliciting knowledge from experts: A methodological analysis," *Organ. Behav. Hum. Decis. Process.*, vol. 62, no. 2, pp. 129–158, May 1995. doi: 10.1006/obhd.1995.1039.
19. M. J. Spector, D. M. Merrill, J. Elen, and M. J. Bishop, *Handbook of Research on Educational Communication and Technology*. New York: Springer-Verlag, 2014
20. M. De Gramatica, F. Massacci, W. Shim, A. Tedeschi, and J. Williams, "IT interdependence and the economic fairness of cybersecurity regulations for civil aviation," *IEEE Security Privacy*, vol. 13, no. 5, pp. 52–61, Sept.–Oct. 2015. doi: 10.1109/MSP.2015.98.
21. M. de Gramatica, F. Massacci, W. Shim, U. Turhan, and J. Williams, "Agency problems and airport security: Quantitative and qualitative evidence on the impact of security training," *Risk Anal.*, vol. 37, no. 2, pp. 372–395, Mar. 2016. doi: 10.1111/risa.12607.
22. M. Halaweh, "Using grounded theory as a method for system requirements analysis," *J. Inform. Syst. Technol. Manage.*, vol. 9, no. 1, pp. 23–38, Apr. 2012. doi: 10.4301/S1807-17752012000100002.

Pierantonia Sterlini (p.sterlini@unitn.it) is a research project manager at the University of Trento, Italy. Sterlini received a B.S. in international studies from the University of Trento. She leads the education and capability work package of the Horizon 2020 CyberSecurity4Europe pilot. She is a past president of the Italian Fair Trade Commercial Cooperative Organization.

Fabio Massacci (fabio.massacci@unitn.it) is a professor at the University of Trento, Italy. Massacci received a Ph.D. in computer engineering from the Sapienza University of Rome, Italy. He published more than 250 peer-reviewed papers and received the Ten Year Most Influential Paper Award at the 2015 IEEE International Requirements Engineering Conference. He coordinated several European Union initiatives, including the Socio-Economics Meets Security project, and he participates with the Common Vulnerability Scoring System Special Interest Group. He is Member of the IEEE.

Natalia Kadenko (kadenko@tudelft.nl) is a postdoctoral student in cybersecurity governance at Delft University of Technology, The Netherlands. Kadenko received a Ph.D. in the political problems of international systems and global governance from the Taras Shevchenko National University of Kyiv, Ukraine. She has worked as an editor and political analyst and cooperated with a nongovernmental organization that specialized in peacekeeping research.

Tobias Fiebig (t.fiebig@tudelft.nl) is an associate professor at Delft University of Technology, The Netherlands. Fiebig received a Ph.D. in computer networks from the Berlin Institute of Technology. A former network engineer, he works with several national and international research programs, including the Horizon 2020 Safe-Data–Enabled Economic Development project, and he leads the governance work package for the Horizon 2020 CyberSecurity4Europe pilot.

Michel van Eeten (m.j.g.vaneeten@tudelft.nl) is a professor at Delft University of Technology, The Netherlands, and the director of the Technology, Policy, and Management Graduate School. His research focuses on the interplay between technological design and economic incentives in Internet security. Van Eeten received a Ph.D. from Delft University of Technology. He led research projects funded by the European Union, Netherlands Organization for Scientific Research, and industry that concerned the economics of cybersecurity and cybercrime. He serves on the Program Committee of the Workshop on Economics of Information Security and is a member of the Dutch Cyber Security Council.