Cyber Security for Europe

Realising Europe’s Cybersecurity Strengths and Capacity for the 2020s

With the friendly support of the Representation of the State of Hessen to the EU

HESSEN

A CyberSec4Europe Online Panel Discussion
19:00-20:30 CEST, 9 July 2020

Introduction and Welcome

Kai Rannenberg, coordinator of CyberSec4Europe, opened the evening by introducing Lucia Puttrich, Hessian Minister of European and Federal Affairs and Representative of the State of Hessen at the Federal Government, who gave a warm welcome on behalf of the Hessen Representation to the EU, our event partner and supporter.

Kai then ‘served’ CyberSec4Europe’s ‘food for thought’ with an overview of the CyberSec4Europe project and its latest deliverables, mentioning in particular those relevant for the panel discussion[1].

Lucia Puttrich at the Representation of the State of Hessen to the EU

Discussion Background

On 12 September 2018, the European Commission proposed a regulation establishing a European Cybersecurity Industrial, Technology and Research Competence Centre and a Network of National Coordination Centres. Its aim was to improve EU cybersecurity and resilience, enhance and strengthen the EU's cybersecurity capacity, stimulating the European cybersecurity technological and industrial ecosystem, as well as to coordinate and pool relevant EU resources. Two years later, key aspects of the proposal continue to be discussed among the major European institutions[2] supported by the four pilot projects, including CyberSec4Europe.

The evening online panel discussion aimed to explore how the proposed Competence Centre and Network regulation will progress during the German EU Presidency which started on 1 July – and beyond.

[1] Deliverable D2.1: Governance Structure and Deliverable D4.2: Legal Framework

[2] The European Council, the European Commission, the Council of the European Union and the European Parliament

CyberSec4Europe is funded by the European Union under the H2020 Programme Grant Agreement No. 830929

The Panel

The distinguished group of panelists were:

- **Tamara Tafra** who since 2013 has been working for the Permanent Representation of Croatia to the EU, covering COEST, COSCE[3] and CYBER. She is currently the Counsellor for Cyber Issues and was Chair of the Horizontal Working Party on Cyber Issues during the Croatian Presidency from 1 January to 30 June 2020.
- **Rasmus Andresen** has been serving as a Member of the European Parliament since 2019 for the Greens/European Free Alliance. After the May 2019 elections, he was appointed Rapporteur for the Cybersecurity Competence Network Centre Regulation dossier. Rasmus is a member of the German Alliance 90/The Greens party.
- **Miguel González-Sancho** is Head of Cybersecurity Technology and Capacity Building, DG CNECT, European Commission.
- **Andreas Könen** has been head of Cyber and Information Security at the German Federal Ministry of the Interior, Building and Community since May 2018.
- **Juhan Lepassaar** has been Executive Director of ENISA since October 2019. After working for several years working with the EU at the Government Office of Estonia, Juhan was Head of Cabinet for Vice-President Andrus Ansip, responsible for the Digital Single Market at the European Commission

The moderator was David Goodman from Trust in Digital Life Association.

The panel, clockwise from top left: David Goodman, Tamara Tafra, Miguel González-Sancho, Andreas Könen, Rasmus Andresen, Juhan Lepassar

[3] COEST (the Council Working Party on Eastern Europe and Central Asia), COSCE (the Council Working Party on the Organization for Security and Cooperation in Europe)

The Story So Far

The panel discussion opened with a high-level review on how the regulation proposal progressed at the Council during the Croatian Presidency which ended on 30 June. Despite the constraints restricting any face to face meetings from March to June, a mandate was agreed by Coreper[4] on 3 June and negotiations with the Parliament started on 25 June, with only two open issues (the number of seats and voting rights). Through the incoming German Presidency, the ambition is to complete the trilogue and to have the regulation adopted by the end of this year. The coming months will see the conclusion of the next long-term EU budget[5] that has to balance funding for the proposed Competence Centre with the requirements of the Digital Europe, Horizon Europe and other programmes.

The Competence Centre[6]

The Competence Centre is intended to be the main body managing EU financial resources dedicated to cybersecurity research under the two proposed programmes – Digital Europe and Horizon Europe – within the next multiannual financial framework for 2021-2027.

During the course of the discussion, a number of interesting points were made, in part stimulated by questions from the (online) audience:

- The primary role of the Competence Centre is to provide investment, identify priorities, both political and technical, pool resources and give support to Member States and the stakeholder community.[7]
- If the governance structure is the Centre's skeleton, its flesh is the actual content, such as planning the Digital Europe programme, engaging with the four pilots and other stakeholders, and getting the involvement of the Member States.
- A number of questions were raised in relation to the anticipated dynamic and engagement of the Member States with the Centre. By example it was suggested that a Member State might express a wish to embark on a particular topic and invite others to make a joint proposal. This could then be taken to the Centre which would approach the EC to match the contribution of the Member States[8].

[4] Coreper stands for the 'Committee of the Permanent Representatives of the Governments of the Member States to the European Union' and is the Council's main preparatory body.

[5] The multi-annual financial framework (MFF 2021-27)

[6] For an overview of the initial tasks and objectives of the European Cybersecurity, Industrial, Technology and Research Competence Centre, see https://ec.europa.eu/digital-single-market/en/european-cybersecurity-industrial-technology-and-research-competence-centre. For a more recent discussion on the structure of the Centre, see Governance Structure; and for the Advisory Board in particular, see ibid, pp. 54-55.

[7] In response to a question from the audience about the European body mentioned in the open consultation on the NIS Directive, it was made clear that this as yet unspecified body is not the Competence Centre. This new body would, for example, be responsible for situational awareness and information gathering of cyber incidents, such as incidents with cross-border relevance and aggregating statistical data. The consultation, which will be open until 2 October 2020, seeks opinions and experiences from all interested stakeholders and citizens.

[8] It was duly noted that, in addition to funding such joint actions, the Member States also underwrite all the ongoing Commission research programmes.

- Also vital is the network the Centre will support, which again includes the pilots as well as the communities associated with ECSO and ENISA. The Commission's Cybersecurity Atlas[9] is already demonstrating how the broader community of cybersecurity experts will be built in practice.

The Advisory Board and the Stakeholder Community

- The thrust of the Council's position is to increase synergies between research and industry and to remove the proposed Advisory Board from the governance structure of the Competence Centre, giving a bigger role to the European cybersecurity stakeholder community with more power to choose their own representatives. In addition, an enhanced role is envisaged for ENISA, ensuring that there is no overlap with the Centre.
- ENISA itself anticipates several levels of cooperation with the Centre – structural, operational (including research area synergies, workshops etc) and a shared community.
- A perceived weakness of the Council proposal is that, if there are only a few people in the Centre making decisions, it would weaken the participation of civil society. Hence, we may expect to see push back from the Parliament on the question of the Advisory Board: it's feared the Council's proposal to remove the Advisory Board would leave the involvement of civil society up to the discretion of the Centre, whereas the Parliament would like the involvement of civil society, industry and science to be kept as an integral part of the structure of the Competence Centre. The intention of both the Parliament and the Council is the same – just a different set of perspectives on how it should be achieved.
- It was confirmed that the concept of CHECKs (Community Hubs of Expertise in Cybersecurity Knowledge)[10], as proposed by CyberSec4Europe, is broadly supported.

Looking Beyond 2020

Finally, the panelists were asked to give their vision for the future beyond 2020:

- The establishment of the Competence Centre will be a step in the direction of giving Europe a stronger and better coordinated role in cybersecurity on the world stage than it has at present, leading to greater European souvereignty.
- A concern was expressed as to whether the Centre will be pro-active, stimulating new products, proposing new legislation and driving standardisation – or 'just' a distributor of money to Member States. Member States are perceived as still prioritising the building of their own cybersecurity capacity, rather than encouraging more money to be invested in common European projects.

[9] See https://www.ffg.at/sites/default/files/downloads/CCCNworkshop.pdf. Piloting of the Cybersecurity Atlas starts in September 2020 with the expectation that it will be open to all stakeholders before the end of the year.

[10] See CyberSec4Europe Deliverable D2.1, Governance Structure and CyberSec4Europe Offers Complementary Input To Cybersecurity Network Governance

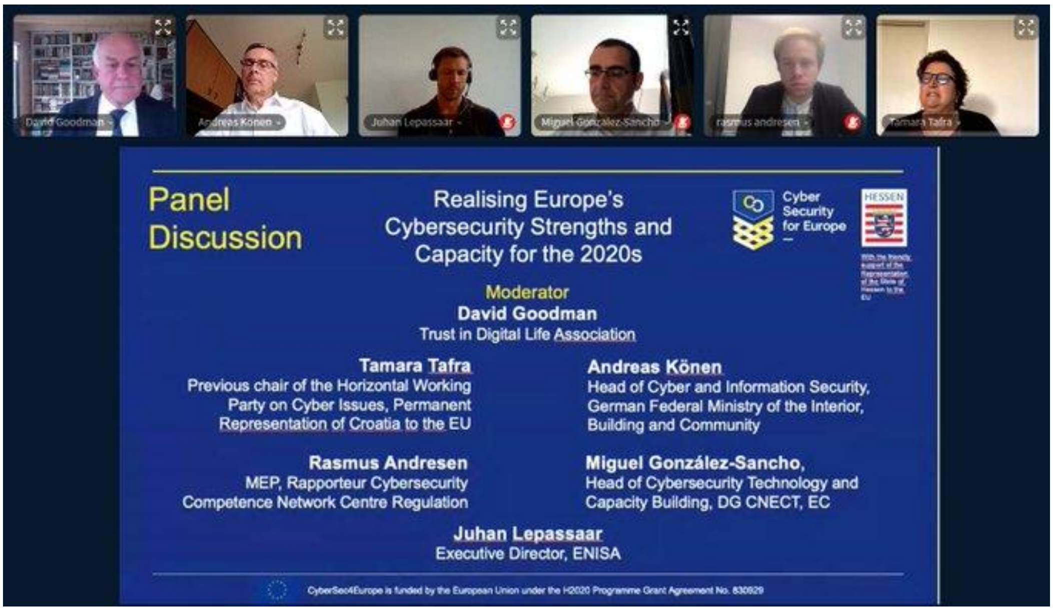
CyberSec4Europe is funded by the European Union under the H2020 Programme Grant Agreement No. 830929

- A potential future key performance indicator for both the Competence Centre and ENISA could be when European citizens trust the security of European products and services.
- As agreement on the eventual form of the proposed regulation is in sight, it's finally time to start work on the substance of the proposal for the Centre and Network and move into delivery mode. Throughout the pandemic, everyone has spent more time online and become more keenly aware of cybersecurity issues, at both a micro and macro level, than ever before. It offers an opportunity to headline cybersecurity, particularly as there have been no prominent breaches, except in healthcare. Nonetheless, there is a huge amount of work not only in terms of awareness, but also education, skills and the provision of resources. The Centre has a significant role in supporting investment in all these areas.
- One of the first things the Centre will do next year is to launch its first round of projects, the results of which we should be able to see – hopefully when we meet again in person at the Hessen Representation in Brussels.

Until The Next Time

In an echo of a core COVID-19 message, it was observed that however much we invest, it will always all come down to the actions of individuals, raising awareness and working on cyber hygiene, in order to protect us all.

CyberSec4Europe thanked the panelists for their candid and insightful contributions; and to the audience who in 3-digit-numbers stayed online and lingered longer than had been expected.



Panel Discussion

Realising Europe's Cybersecurity Strengths and Capacity for the 2020s

Moderator
David Goodman
Trust in Digital Life Association

Tamara Tafra
Previous chair of the Horizontal Working Party on Cyber Issues, Permanent Representation of Croatia to the EU

Andreas Könen
Head of Cyber and Information Security, German Federal Ministry of the Interior, Building and Community

Rasmus Andresen
MEP, Rapporteur Cybersecurity Competence Network Centre Regulation

Miguel González-Sancho,
Head of Cybersecurity Technology and Capacity Building, DG CNECT, EC

Juhan Lepassaar
Executive Director, ENISA

CyberSec4Europe is funded by the European Union under the H2020 Programme Grant Agreement No. 830929