Community perspectives on the future of cybersecurity in Europe

As plans for the European Cybersecurity Competence Centre and Network are being fulfilled, the wider cybersecurity community continues to play an important role in helping to shape requirements and processes.

On the evening of 18 November 2021, CyberSec4Europe, with the friendly support of the Representation of the State of Hessen to the EU, hosted a roundtable, at which national cybersecurity community representatives from across Europe shared their experiences, challenges and their aspirations for the future of cybersecurity in Europe.

Each Member State has its own set of cybersecurity-related priorities or agenda relevant to the specific strengths of its key sectors, many of which have a common set of challenges. Of particular interest is the degree of connectedness of the communities with each other, both at national and supranational levels, which plays into expectations relating to the governance and decision-making processes of the national coordination centres and their relationship with the new European Cybersecurity Competence Centre in Bucharest.

During his welcome address, **Mark Weinmeister**, Secretary of State for European Affairs of the State of Hessen, observed how Europe was facing a diversity of issues, challenges and opportunities in cybersecurity, and that every Memebr State, region and municipality has its own approach and priorities. There are incredible opportunities in this diversity and for it to succeed we need a common framework, working together to fulfil the initiatives coming from the EU and the EC.

Following him, we were privileged to have as keynote speaker **Miguel González-Sancho**, Head of Unit, Cybersecurity Technology and Capacity Building, DG CONNECT, European Commission who is also acting executive director of the Bucharest Centre. Miguel picked up on the two themes of diversity and a common framework, and added a third – priority, all of which added up to what the regulation on the Cybersecurity Competence Centre and Network are about – a governance proposition. Miguel highlighted the three-layer model – the Centre, the national coordination centres and the community – and reflected how the regulation was inspired by the wider community and their expertise and will continue to interact as an information feed for strategic and funding decisions from the top. To give an update on progress to date, Miguel informed that:

- The Governing Board of the Centre (ECCC) with representatives from all Member States and ENISA, as a permanent observer, met on 20 October to discuss matters of substance.
- The Member States have until 29 December to put forward their national coordination centres (NCCCs). One of the vehicles to support the NCCCs will be the Digital Europe programme which was officially adopted in November and will be opened in February ’22 with another round later in the year. The EC met with the Member States on 28 October to discuss the services and mission of the NCCCs, including how the communities can become involved and to share willingness to exchange cross-border to facilitate collaboration.
- The community is diverse and is represented at both national and supranational levels. For example, ECSO has developed its scope of work with the EC and the four pilots, of which CyberSec4Europe is one, have a vision of structuring and coordinating the cooperation – as exemplified by this evening’s event.

Miguel concluded by reminding us that, even though the cybersecurity community has vision, there is a certain degree of fragmentation. Hence, the need to raise up to threats

and opportunities to realise the potential, identifying and implementing priorities as well as leveraging expertise with funding.

The roundtable moderator, **David Goodman**, the Senior Consultant at Trust in Digital Life, invited each of the participants to introduce themselves and briefly share their challenges and expectations in the light of what they'd heard from the keynote speaker.

- **CyberSec4Europe – Natalia Kadenko** is a postdoctoral researcher in Cybersecurity Governance and Disinformation at TU Delft and is leading the project work that is looking at the Governance model for the cybersecurity community network.
- **Italy – Matteo Lucchetti** is director of CYBER 4.0, a private-public partnership and one of eight competence centres set up by the Italian ministry, each with their own objectives and mission. Their target is mostly public administrations and SMEs and are aware of the lack of competencies that need to be addressed in a systematic fashion. Their constituency includes, as well as the largest cybersecurity companies in Italy, several universities and training institutions – a vital resource in offering upskilling and reskilling to those on the front line. Their main activities are in capacity building, orientation towards the market and the promotion of research and innovation projects. They are eager to contribute to the ECCC and the sustainability of competence building across Europe.
- **The Netherlands – Eddy Boot** is director at dcypher, a collaboration platform for cybersecurity innovation, which is an independent public-private partnership, set up by the Ministry for Economic Affairs and Climate as will be the forthcoming NCCC. The issues and challenges they come across are similar to those found in Italy. Starting from academia, the chain from small to large, the valorisation is difficult. The overall ambition is to increase expertise in the Netherlands.
- **Germany – Christian Mrugalla** is Head of Division, International Cybersecurity and Cybersecurity Research at the Federal Ministry of the Interior. In Germany, the NCCC is going to be set up in the public sector (in the BFI) with the collaboration of several stakeholder ministries. He commented that there is a lack of good networking between different sectors, but too much dependency on 'far away countries' which raises the issue of European digital sovereignty: it's difficult to rely on Europe alone for new technologies, such as 5G: too often we have lost leadership. Europe needs to be better with its research activities and the involvement of SMEs. Christian sees addressing these issues, among many others, as the main task of the ECCC.
- **Spain – Juan Díez González**, Head of support to research and innovation at INCIBE, the Spanish National Cybersecurity Institute which is already doing many of the things a NCCC is expected to do. The support from ECSO and the four pilots have an important role to play in the wider European community and has a role to play in providing guidelines, recommendations and commonalities for Member States that are useful in the context of the regulations. The Spanish national cyber strategy provides an operational instrument – an invitation-only diverse national cybersecurity forum – that is working closely to support regional communities.
- **Greece – Ioannis Alexakis** is Head of the Directorate for Cybersecurity Strategic Planning in the General Secretariat of Telecommunications and Posts at the Ministry of Digital Governance. They are collaborating with communities in Greece and working on the creation of a national cybersecurity strategy, having

strong relations with major industry hubs in the main cities. Digitalisation in public bodies, industry and SMEs have more recently become a major priority, and that includes the importance of cybersecurity research and awareness in their daily operations. They are looking for support to their NCCC from the ECCC to help with capacity building and community building.

- **Norway – Silje Johansen** is an advisor at the Norwegian Digitalisation Agency, responsible for following cybersecurity under DIGITAL Europe. Norway is not yet fully associated with the Competence Centre regulation but hopefully it is just a matter of time. Silje's organisation is looking at the gaps and the needs in order to be prepared. Their main activity is bringing results from research to the market and experience many of the same issues as the other community representatives have observed. One of the strengths in Norwegian digitalisation is that there is a high level of trust from the public in the public sector, with very good identity and authentication services which is a starting point for developers to use. One of the hopes or expectations from the community is learning how to overcome the gaps as well as being able to reach out to SMEs. There really is a demand to communicate between research and industry and SMEs and it is hoped that a future NCCC will fulfil that role.
- **Ireland – James Caffrey** is a staff engineer in the Cyber Security & Internet Policy Division in the Department of Environment, Climate & Communication. He pointed out that for many reasons Ireland is Anglo-centric and is at home working with third countries, which can be a key challenge in terms of cohesion in a European context. A national cybersecurity challenge would be expected to look at protect – develop – engage. Ireland sees key challenges with the regulation as it takes an open global approach for opportunities. It needs to be outward-looking and is very keen to see international cooperation continue. It sees the importance of building up indigenous capabilities but so is working together trans-Atlantic, preserving its open economy as is demonstrated by the large number of international companies based in Ireland. This gives a different approach to digital sovereignty and presents key challenges in networking, building bridges, and getting to know one another. What is the Irish national cybersecurity community – it's highly fragmented and competitive. Europe is not a great exporting bloc and it needs to realise that. We are not at the cutting edge in many areas – we need to be clear about the agenda. James felt that Europe lacks a common vision and common understanding on policy and industry engagement and sees the need for different levels of autonomy. For the future NCCC, he sees a strong role for policy, industry engagement and development and to some extent enterprise support but there are still a lot of questions and challenges.

Having completed the tour de table, a question from Antonio Skarmeta from the University of Murcia was put to the participants:

> *When you're thinking on communities, were you thinking on individual entities or are you also considering regional communities or even sectoral communities, and what could be the impact on governance of a national community?*

Silje stated that in Norway the highest technical competence in cybersecurity is situated in the research community, basically universities and research institutes, as well as the public sector where it is very concentrated in, for example, cyber range and certification. Another challenge is that there are extreme sectoral divides in the public sector where everyone has their own very

clear mandate. So, when they think about community, it's very much sector related.

Christian emphasised the importance of the governance role of the ECCC in bringing together these communities. Far more pertinent though is building up trust, not between organisations, but between people which would have been enormously difficult to include in the regulation. Building up trust between the actors is of paramount importance, not least in being able to exchange ideas.

Natalia followed with a question as to what would be the appropriate tool or instrument to facilitate such trust, for example, registered community members – can we be more pro-active or is this just going to lead to unnecessary complications?

Christian agreed that we needed both – a listing or registration process to get the kind of communities we really want. We should not overestimate this, bearing in mind some of the discussions about aspects of the regulation being overcomplicated enough. Personal contact through working groups and meetings is the only way we can really build up trust – sharing the same goals and experiences about challenges and goals.

James replied that we need a common baseline, we need to know each other but on the other hand if we have a registration process, what's the benefit for joining, what would be in it for a researcher? These benefits need to be clear and self-evident and representative of the stakeholders on the ground. We have to see more outreach, more networking – only with more engagement that we're going to get to know each other in order to collaborate effectively. Brussels has a reputation of being bureaucratic and a bubble which is difficult to break into from outside, particularly if you are an SME or an indigenous player. He also highlighted that there are thousands of European citizens working for multinational companies whose expertise we should make good use of. Overall, we need to bring people together. This has to happen at all levels – the regulation, the national conversations or something much more fluid in terms of building cohesion.

Finally, **Juan Diez** highlighted the important role that ECSO and the four pilots can contribute in terms of whitepapers and guidelines to help and support the emergence of the NCCCs. **Natalia** mentioned that the four pilots are already working on such a whitepaper and would be happy to receive more information from the communities to complete the work.

As the discussion drew to a close, **David** invited **Miguel** to sum up his reaction to the points raised by the roundtable participants. Miguel emphasised the structure embodied in the regulation which were designed to address many of the challenges raised by the communities. The framework and the NCCCs in particular have a remit to accommodate the wide diversity of experience and expertise across the wider European cybersecurity community and through a common agenda ensure that all voices can be heard. The role of the Commission is to facilitate this collaboration.

Community perspectives on the future of cybersecurity in Europe