ENISA HIGH LEVEL INDUSTRY DINNER AND EVENT

MEETING REPORT

MEETING MINUTES

LOCATION BAVARIAN REPRESENTATION TO THE EU, BRUSSELS

DATE 11-12 JUNE 2019

EXECUTIVE SUMMARY

ENISA, in cooperation with the Bavarian Representation to the EU, organized a high level industry event focusing on the future of cybersecurity for Europe. Several key stakeholders in EU cybersecurity shared their views and discussed challenges and opportunities by looking to both the past and the future. The key messages of the event are the following:

- Cybersecurity in the EU needs continuous attention from politicians, policy makers, industry, and academia. This should lead to a constructive discussion about the risks and possibilities of cybersecurity within the EU context.
- The EU is one of the world leaders in the development of the digital society. This is mostly driven by regulations such as GDPR, ICT Certification, eIDAS and NISD. It should improve capitalizing this global advantage and translate it into business opportunities. Here lies a role for both the European Commission, Council (Member States) and industry.
- Digital sovereignty in the context of cybersecurity, and against recent developments in the global tech environment, should continue to be discussed and lead to a firm stance of the EU and its member states. A common and shared understanding of its scope and objective is needed, followed by a possible plan to achieve digital sovereignty. The industry looks to ENISA to discuss this with the new European Commission, to inform the newly elected European Parliamentarians, and in general to facilitate this discussion on a European level with relevant stakeholders.

BACKGROUND

The outcome of the EU elections offers a chance to support the (re-)elected politicians with a consolidated view on the cyber challenges the EU faces today, and to provide them with clear solutions on how to address them while pointing to opportunities for strengthening the European ICT industry. In its role as an expert organisation in cybersecurity, ENISA is ready and willing to support this process.

In cooperation with the Bavarian Representation in Brussels, ENISA organizes 2 events to serve as input for the newly elected Parliament and Commission:

1. An event on 12th June (dinner 11th, “by invitation” only due to limited space) in Brussels to look forward to the Cybersecurity needs for the future. It is expected that the output of this meeting will serve as input for the newly elected Parliament and Commissioners to address these challenges. This fora is scheduled to take place on 24 September;

2. An MEP breakfast on 24th September to discuss the output of the June event is presented and discussed. ENISA shall bring the conclusions of the MEP meeting, together with the input from the previous event, to the attention to the newly elected European Commission.

INDUSTRY DINNER, 11 JUNE 2019:

ENISA invited the speakers and panellists for an opening dinner, and included a selection of its key stakeholders to join. It resulted in a dinner consisting of nearly 30 well placed 'influentials' in the EU cybersecurity industry, academia and government. The purpose of the dinner was to introduce the topic and engage the dinner guest in a dialogue on the road forward. The following key points have been made:

- The EU cybersecurity market has great potential, as the EU produces many talented and skilled experts. It should be more attractive for talent to continue and pursue their career within the EU, preferably for EU companies. Some guests even argued that the EU is underperforming in keeping and nurturing SMEs. We need to invest in excellence.
- Cooperation, information and knowledge exchange between the public and private sector is important to break the fragmentation
- One of the remaining obstacles of the Digital Single Market continues to be language barriers. As an example, Irish or British start-ups/SMEs are more inclined to look to the US than to the EU.
- Multiple guests called for a stronger industrial policy. But the focus of such a policy remained unclear throughout the discussions: to support the economy, to support the industry, to ensure digital security, etc?
- Both industry and governments should investigate in how to create a better market environment for funding within the EU DSM, leveraging the geographic and community harmonisation.
- One main issue remains the administrative burden for entrepreneurs in the EU. In the US this is much easier, but they generally take more risk.
- The EU has too many SMEs, we need more larger companies in order to create the motors of development and industry strength.
- One of the great successes of EU leadership in regulation in recent years is the development and implementation of the GDPR. It demonstrates that the EU is not at all behind in the tech-race, but has its own vision. A vision that has to be copied by the rest of the (digital) world powers. The EU can use this as a positive driver for changing its vision focusing on strength and growth via regulation power.
- Many guests took the opportunity to connect their views to the future role of ENISA:
    - ENISA as the facilitator of getting communities together (Industry, Commission, Member States, Academia). There is too much fragmentation in order to make a strong fist against American and Chinese ICT industry. Another argument for a stronger coordination role is that ENISA should facilitate more cooperation among regulators and policy makers (Commission/Member states) before regulation is developed and implemented.
    - ENISA should enhance its operational power to live up to its expectation as the EU Cybersecurity Agency;
    - ENISA needs to move away from an advisor role into a leading role on cybersecurity in the EU, and beyond. From a EU perspective that means ENISA should be consulted on any piece of legislation that involves cybersecurity, with the power to reject based on its expert role.
    - ENISA should promote its work more and wider. Its studies and reports are not 'sold' well enough.

ENISA HIGH LEVEL INDUSTRY DINNER AND EVENT

MEETING REPORT

INDUSTRY EVENT, 12 JUNE 2019

The event was divided in (1) providing challenging views to the audience, followed by (2) a panel that includes speakers to discuss the previous interventions and identify a vision for the cybersecurity community to go forward.

Impulse speeches:

ENISA invited Facebook, the UK Government, Alliance pour la Confiance Numérique, BH Consulting, and the CODE Institute to share their views in 10 minutes impulse statements.

- The interventions by Facebook and the UK government focused on the societal aspects of social media by discussing possible regulation frameworks, cybersecurity attacks on social media, the responsibility between public and private, and the positive and negative effects of technology development on our digital society. According to both parties ENISA can fulfil a cybersecurity expert role in these sensitive and necessary discussions.
- Alliance pour la Confiance Numérique (ACN) provided a perspective on the Digital Single Market and the competitiveness of the EU on the global cybersecurity market. ACN believes the EU market is too fragmented to be competitive with the Asian and US market. At the product development level, SMEs are investing too much in similar topics or products. We need more innovation in the cyber market. Larger EU companies need to collaborate more with SMEs on an EU level to overcome the boundaries. Here the EU can assist the industry, because there is no long-term strategy. ENISA should jump in this gap to invest in facilitating collaboration, discussion, and ultimately gain a coordinating role that supports the development of the EU cybersecurity market and its competitiveness.
- BH Consulting, an SME from Ireland active in the EU and outside the EU, presented a business perspective on both the opportunities and risks involved in cyber threat intelligence. This generation has the responsibility to design and implement a secure and safe internet environment, amidst all the destabilizing factors trying to prevent this. As an SM, BH Consulting, looks to better law enforcement in terms of stronger regulation, more education, and increasing the cyber expertise within.
- The CODE Institute (Universität der Bundeswehr München) shared its views on the role of research and innovation. There is great research being conducted in the EU, the issue is that there is no follow up. This gap needs to be closed. Our chance is now to connect the relevant players on the EU market of research and innovation. One example is the EU subsidised program that involves Concordia, Echo, Sparta, and Cybersec4europe. These pilots that aim to invest in coordinating cyber competences and expertise could provide solutions and best practices to tackle this challenge. With the rise of fundamental issues such as the security of 5G, the EU needs to discuss digital sovereignty. Building eco-systems in the EU is a great first step to achieve this.

Panel discussion:

ENISA invites Symantec, BEUC, Rohde & Schwarz, and Secunet to share their views and engage in a discussion on the future regulatory agenda for the European Parliament and the Commission. The following key messages and discussion points were defined:

- In response to the European discussions on the role of SMEs, the EU should invest more in its larger organizations/multinationals to run large-scale projects, and by doing so, involve the SME community;
- Faster deployment of projects and products is essential, our processes to innovate and produce need to speed up rapidly;
- The role of consumers is absent in the regulatory frameworks dealing with cybersecurity. A safety net for consumers is necessary; consumers need to understand what they buy.

- The EU lacks a clear strategy because it avoids making (difficult) choices. Look for the niches and opportunities of cybersecurity, and identify the areas where the EU has the upper hand. Then start strategizing from a position of strength.
- The development of regulation such as GDPR, Certification and even the NISD are great examples of the leadership role of the EU. It also demonstrates that industry develops itself around such regulation.
- One of the main conclusions is that the next European Parliament and Commission, involving the Council, should aim for a political and strategic discussion on the digital sovereignty of the EU. What is the scope? Are all member states interested in investing in it? What about the industries? How should the EU approach it? From economic, political, societal, and/or democratic values? What would be the clear objective of such a discussion?

CONCLUDING REMARKS AND FOLLOW UP

The ED of ENISA provided the audience and speakers with a few conclusions and advise for the future:

- Continue and invest in the constant dialogue among civil servants, industry, and politicians
- EU Digital Sovereignty is essential for the development of EU cybersecurity
- Find the right balance between EU expert institutions, the Commission and Member States. The model needs to be driven by complementarity based on independent roles.
- ENISA is stronger connected to EU regulation (NISD, Certification framework, etc). Its stakeholders need to be able to profit from this change and question if that is not the case.
- ENISA's current strategy ends in 2020, therefore a new strategy needs to be developed. Here ENISA welcomes input from its stakeholders.

On 24 September 2019 ENISA organizes, in cooperation with the Bavarian Representation, a breakfast for MEPs. At this breakfast it will introduce the same issues, and will include the key messages of this industry event. The outcome of that discussion with the MEPs will lead to a better understanding of the necessities and possibilities of cybersecurity in the EU. The final conclusions will be discussed with the European Commission as input to the next term.