Cybersecurity in Europe – research, industry and innovation opportunities

On Friday 9 September 2016 creoDK together with Aalborg University and the Confederation of Danish Industry held an event on Cybersecurity in Europe. The aim was to outline research, industry and innovation opportunities in conjunction with the EU cyber security contractual Public Private Partnership (cPPP) launched by the European Commission and European Cyber Security Organization (ECSO) in July.

The day was opened by Anette Broløs, the CEO of CFIR. In her introductions Broløs noted with a broad array of speakers (16 in total) and many signed up for the event (around 85) there was scope for moving the discussion forward in an area where she stressed not only general support but further hard work is still required. Broløs also made the point that the event proved Denmark performed on the gender balance in this field.

In an inspiring and spirited introduction Professor Fritz Henglein from DIKU outlined some of the cyber issues at stake – with thought provoking references to the future being bright if you are an optimist, but attacks, malware and vulnerability exist. Often action is only taken after damage is done, as no natural market exists before. Attack vectors include social engineering, insecure software and privacy attacks. Henglein finished by outlining Danish strongholds that can help Denmark contribute to cyber security, even if one cannot claim Denmark is cyber secure as such.

The event then turned its attention to the **EU actions with two key notes speakers**. First, Luigi Rebuffi, SG of European Cyber Security Organisation (ECSO) described the purpose and structure of the cPPP in some detail. Rebuffi noted that due to the sensitive nature of the issue, the cPPP quite unusually also have Member States included in the governance structure. Currently Denmark has no members. The budget for the cPPP is €450m over four years with an intended leverage factor of 3. The overall message was one of a tight timeline, with several parallel work tracks covered with 6 working groups (1) Standardization & certification, 2) Market development, 3) Sectoral demand, 4) SME support, 5) Education & awareness, 6) Technical areas/products/services). The first meeting of the ECS takes place within weeks.

Secondly, Jakub Boratynski the HoU responsible for Cyber Security and Digital Privacy in the European Commission's DG CNECT, who supplemented the PPP presentation with focus on the other actions taken and foreseen by the Commission – these included quite naturally the recently adopted NIS directive, but also forthcoming efforts/proposals to upscale investments, a possible certification scheme and an enhanced mandate for the ENISA agency. The Commission warned that the EU is not really ready for a major attack and cooperation in not yet strong enough, hence more work is foreseen. The Commission was considering a

contest in the first quarter of next year on seamless identification. Boratynski stressed that participation in the cPPP is not only an opportunity for influencing the research and innovation in the area, but also an opportunity to influence the thinking of the Commission.

There were a number of questions to both speakers regarding the funding of the PPP, ways to participate, SME possibilities, and the success of H2020 to date, etc.

A first **panel discussion on data protection by design** was chaired by Professor Søren Sandfeldt from AAU, who led the panel into a discussion of how to create optimal conditions for creating research driven data protection industry in Europe and if the seemingly simple idea of building in software from the onset is indeed feasible. Professor Lars Bo Langsted from AAU stressed that international law is constantly changing, meaning not only technical but also legal research is required when developing new solutions. Lawyer Camilla Bonde from AAU explained an important prerequisite is strong regulators that are independent of governments. CTO Jakob Pagter from Sepior pointed to their positive experience with funding from the EU SME instrument (Sepior in 2015 received the venture capital), and CTO Jacob Herbst from Dubex stressed key elements are usability and functionality for consumers.

A lively discussion within the panel and with the floor raised issues such as what lawyers can contribute with, the benefits of soft law versus hard law framework, what types of access is required, the difficult task of balancing usability and protection, and whether a backdoor for authorities is feasible without leaving it open to others.

A second **panel discussion on Internet of Things security** was led by IT security specialist Charlotte Miolane on the questions of how to gain a competitive edge security for the future. Professor Knud Erik Skouby from AAU opened the discussion outlining how detailed decision making in all situations is too cumbersome, hence silent computing is useful, but has to be balanced with consumer control. Skouby also provokingly noted that if IoT security is not put in place now for the 5G platform, it will be too late – concluding it is high time for, and appropriate with, a EU level action. Anders Mynster from DELTA spoke on the basis of his experience with electromagnetic compatibility, with reference to existing legislative EU framework and a vivid exemplification of controlling a forty foot crane lifting a container. Mynster wanted simple elements such as password encryption dealt with before more advanced systems. Associate professor Christian Probst from DTU Compute acknowledged that the security field is difficult to test to the same level as engineers can

check building elements, whilst Herbst on his part stressed the difference between normal product safety and cybersecurity, where intelligent attackers seek to create deliberate failures.

The panel was not all in agreement on these statements and briefly veered into a more general cyber security discussion. Further questions from the floor brought the debate back to IoT, where speakers proceeded to suggest further development of for instance one button/device connected to different things, depending on locality, and systems for lifecycle updates beyond expected lifetime of products.

Making things more tangible the last section switched focus to **two concrete spinout companies**. The CEO of Dencrypt, a company which has been developed in cooperation with DTU, described their claim to a better way of doing encryption via a dynamic encryption principle and outlined some of the immediate benefits of being a spinout. The CEO of Partisia described its ongoing development of a commercial platform, with no single point of trust but rather a distributed system.

Summarising key messages and providing the closing remarks Katrine Nissen HoU of the policy division of the Danish Agency for Science, Technology and Innovation noted the event had demonstrated presence of both potential and engagement, whilst more solutions were needed. The Agency representative urged for Danish research and businesses to take part in the EU initiative, whilst on their part committing also to look into what can be done from the side of authorities in support of this back bone of modern society.

Coffee breaks and a sandwich lunch in the course of the day offered good opportunities for networking in the margins at Copenhagen University, Alexandersalen.

The event was announced on websites of AAU, creoDK and DI, and tweets were communicated before and during the event – using **#CyberSecurityinEU.**

A very big thank you to both the long list of speakers and interested and active participants from all of us!

AALBORG UNIVERSITY DENMARK

UNIVERSITY OF COPENHAGEN

DI Digital

creoDK