Participatory Webinar and Policy Brief on Cybersecurity and its impact on EU-US ICT collaboration

Introduction and Scope

The PICASSO project organised a participatory webinar on **"Cybersecurity and its impact on EU-US ICT collaboration".**

With this webinar, PICASSO brought forward policy recommendations designed to improve EU/US ICT-orientated collaborations – specifically in the technological domains associated with 5G networks, Big Data, and IoT/CPS with focus on the implications of technological developments for cybersecurity policy, taking into account the different approaches towards cybersecurity being taken in the USA and in Europe, the technical and socio-economic backgrounds and new developments likely to affect the security and vulnerability of ICT systems.

Background Notes

The participatory and interactive webinar sought to validate and further develop initial conclusions based on a draft Policy Brief on Cybersecurity and its impact on EU/US ICT Policy collaboration prepared by the PICASSO ICT Policy Expert Group. The Policy Briefing shall be updated with content from the webinar discussions and beyond and published shortly.

Agenda

PICASSO Welcome and purpose of the call
Maarten Botterman, PICASSO Policy Expert Group Chairman

Introduction to EU-US Cybersecurity technology issues relating to ICT development
Dr. David Farber, Carnegie Mellon University, IEEE fellow, ACM fellow

Introduction to EU-US Cybersecurity policy issues relating to ICT development
Dr. *Jonathan Cave, GNKS Consult and University of Warwick*

Introducing the three domains - 5G, Big Data, IoT/CPS
Yaning Zou, PICASSO 5G Networks Expert Group Manager
Dr. Nikos Sarris, Chairman of the PICASSO Big Data Expert Group
Christian Sonntag, PICASSO IoT/CPS Expert Group Manager

Open discussion about ICT security aspects of the three domains
Moderated discussion**.**

Organizing Committee

Policy Expert Group Chair: *Maarten Botterman*, GNKS Consult, The Netherlands

Policy Expert Group Member: *Jonathan Cave*, Warwick University, United Kingdom

Marta Calderaro, APRE, Italy

Margot Bezzi, APRE, Italy

Topic leads

5G Networks:

Yaning Zou, Technische Universität Dresden, Germany

Big Data:

Nikos Sarris, Athens Technology Center, Greece

IoT/CPS:

Christian Sonntag, Technische Universität Dortmund, Germany

Technicalities

Webinar Date: 16th May 2017

Duration: approx. 90 minutes

Participation: Free of Charge

Technical System: Adobe Connect

Recording, Presentations and Policy Brief at:
www.picasso-project.eu

PICASSO has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N° 687874.

Participatory Webinar and Policy Brief on Cybersecurity and its impact on EU-US ICT collaboration

Webinar Results

Participants discussed the basic concept of ICT security with a specific focus on 5G Networks, Big Data and CPS/IoT. Participants included spokespersons from all 4 PICASSO expert groups and a number of other experts from research, business, and civil society. Overall more than 90 participants registered to the participatory webinar.

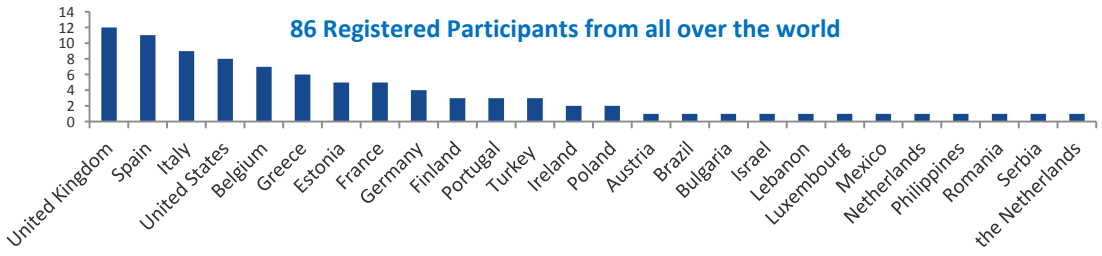
The growing incidence of adverse and highly-publicised events, including massive distributed denial of service attacks on the Internet, malware, hacking, and unauthorized penetration of critical services and sensitive data has disrupted networks, compromised privacy, threatened national information security and noticeably affected policy. The world-wide WannaCry attack the week before the webinar made it increasingly clear to the wider public that events in the cyber and 'real' worlds are directly and tangibly linked; for example, British hospitals were forced to cancel or postpone planned procedures and global costs from this single attack are forecast to exceed $4 billion. There is no magic cure for these serious and endemic security issues. Network security is not confined to the technical layer, but spreads to all layers and beyond to the user community. Progress made in one domain can be undermined by contagion or reinfection from others. The challenges are global and need to be addressed head-on by all stakeholders.

Cooperation on ICT security issues that involve personal data is complicated – on the legal side – by the EU's fundamental right of personal data protection vs. primarily economic nature of US data rights.

- With regard to 5G networks, the main challenges will be escalation and fragmentation; development is producing a hyperconnected world that makes a very attractive target for good and bad behavior, while network slicing makes it possible to define different logical networks with distinct own levels of security;.
- With regard to Big Data, the challenge is to secure data against unauthorised access and tampering. At the same time, big data analytics can help with early detection and prevention of attacks and breaches.
- With regard to Cyber Physical Systems and Internet of Things, there is a further element of complexity; participants noted the need for a security taxonomy for development of ICT based technologies and services and pointed out that outdated security models need to be adapted to become more proactive, and more inspired by biology.

Main Conclusions

It is clear that national agendas are dominated by cybersecurity challenges and 'security mindsets', which make it difficult to work together on contentious issues. At the same time the agendas are converging. There was broad endorsement across domains and territories, for a security and safety taxonomy of objects and services.
Furthermore, progress must be based on the recognition that "old" hardware, software and ways of thinking remain active and cannot be designed away or upgraded out of existence. Strengthening the core of the Internet to facilitate its evolution seems to be an obvious step in enabling a systemic transition towards more dependable applications.



PICASSO has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N° 687874.