PICASSO POLICY BRIEFING 2 (draft input to webinar)

Cybersecurity issues Affecting EU-US ICT Collaboration

On January 1st, 2016, the project PICASSO was launched with two aims: (1) to reinforce EU-US collaboration in ICT research and innovation focusing on pre-competitive research in key enabling technologies related to societal challenges - 5G Networks, Big Data and the Internet of Things/Cyber Physical Systems; and (2) to support EU-US ICT policy dialogue related to these domains with contributions related to e.g. privacy, security, internet governance, interoperability and ethics.

PICASSO is oriented to industrial perspectives and provides a forum for ICT communities. It is built around a group of 24 EU and US specialists, organised into the three technology-oriented ICT Expert Groups and an ICT Policy Expert Group and working closely together to identify policy gaps in or related to the technology domains and to recommend measures to stimulate policy dialogue. This synergy among experts in ICT policies and in the three ICT technology areas is a unique feature of PICASSO.

During its first meeting on 20 May 2016 in Washington DC, hosted by the Department of Commerce, PICASSO experts and other experts focused on identifying key issues in each focus technology area (5G, Big Data, IoT/CPS) and on those policy issues that influence and are influenced by all of these domains. In its first meeting, the ICT Policy Expert group focused on Privacy and Data Protection, recognising that these issues are entangled with all PICASSO-related ICT developments across the Atlantic, directly affecting ICT collaboration. Whereas technology can help addressing policy/societal challenges in ways that have not been possible before, it also poses new challenges for policy/society that need to be considered. In particular the real and perceived policy differences between the EU and USA may make it more difficult for ICT researchers to collaborate towards technology and technology deployment solutions that are suitable for both US and EU markets. In this, there is a role for commerce, business and the economy, since economic methods and motives drive both policy and technology, as well as provide their own forms of problems and solutions.

Amongst its activities, the PICASSO Policy Expert Group is organising a series of webinar to share its reflection with selected experts. The present briefing is meant to provide input for a second webinar, inviting all three thematic expert groups (5G, Big Data, IoT/CPS) to join us in reflecting upon the reciprocal impacts of cybersecurity matters on their specific areas of expertise.

This is the second of 5 thematic Policy Papers and accompanying Webinars that will take place over the coming two years. The first one took place in October 2016 and was focused on Data Protection. Future subjects for Policy Papers will be Standardisation; Spectrum; and one to be decided – currently “Smart Cities”. The intent is to get a clear overview of the most pressing and/or challenging policy issues that confront technological, business and policy collaborations, and to develop valid and practical insights into how these can be addressed from a transatlantic multistakeholder perspective operating in a global context.

Please feel free to share your thoughts via email to maarten@gnksconsult.com.
Looking forward to engaging with you all,
Best regards

Maarten Botterman
Chairman Policy Expert Group
PICASSO project

Dave Farber
Co-Chair Policy Expert Group
PICASSO project

CYBERSECURITY (draft outline)
and its impact on EU/US ICT Policy collaboration

One objective of the PICASSO project is to bring 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. One of the biggest challenges concerns cybersecurity – a subject that touches us all yet with a specific role for governments in terms of the monopoly for upholding the law, and recognising the increasingly-fraught bone of contention in the government sphere, where national governments and supranational governance entities tussle over criminal justice, national security and other vital national interests.

These technological domains overlap in the technological, economic/commercial, business and societal planes. Each of these dimensions creates a shared perspective on the common problems and thereby serves as a platform for internal as well as cross-plane (multistakeholder) interaction. Problems, issues or challenges may have their causes in one (set of) planes, their effects in another and their solutions in a third. Therefore, the interactions (here called 'collaborations') combine collaboration with competition. Concretely, cybersecurity issues will need to be addressed by a combination of various technological, economic and policy measures. Whether EU/US collaboration leads to a technological, economic, regulatory or societal 'solution' will depend on a competitive struggle (across markets, labs and legislatures) as much as it does on a cooperative, neutral and civilised discussion. This mix of modes (cooperation, competition and conflict) can clearly be seen in practice every day.

Although PICASSO will not be able to fully address all stakeholder concerns, it aims to explore how US/EU collaboration in ICT can best be served, taking into account the differences in approach towards cybersecurity in the USA and in Europe, respecting the law and citizens' expectations and preserving the widest possible scope for innovation and deployment.

This paper is based on the draft outline policy briefing on Cybersecurity to the PICASSO ICT Policy Expert Group, and serve as input to the first Policy PICASSO webinar that will be held on 16 May 2017 (starting at 15:00 UTC).

Outline summary (draft)

On January 1st, 2016, the project PICASSO was launched with two aims: (1) to reinforce EU-US ICT research and innovation collaboration, especially pre-competitive research in key enabling technologies related to societal challenges - 5G Networks, Big Data and the Internet of Things/Cyber Physical Systems; and (2) to support EU-US ICT policy dialogue related to these domains with contributions related to e.g. privacy, security, internet governance, interoperability and ethics.

This policy paper focuses on cybersecurity policy considerations in the EU and the US that particularly affect and are affected by ICT research and innovation collaboration related to 5G Networks, Big Data, and Internet of Things/Cyber Physical Systems.

Cybersecurity is high on the agenda of policy makers throughout the world. 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 seriously disrupted networks and compromised privacy and national information security.

There is no magic cure for the serious security issues that that have become endemic throughout the underlying infrastructures and services that have become so fundamental to the way we communicate, access information, and interact. And even more so: each 'cure' sets the stage for the next set of 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; governments who have the monopoly on the coercive power of the law, end users who must act knowledgeably and responsibly, ICT developers who are responsible both for security 'by design' and for critical vulnerabilities and businesses using and/or deploying ICT and ICT-based or –enhanced services in more or less responsible ways. A proper balance between responsible action by individual entities and collaboration among stakeholders is essential if sustainable progress is to be made.

In this paper we will first describe the current technical situation, to provide what we hope is a useful perspective on todays' vulnerabilities of communication and IT systems and the worldwide Internet. Technical complexity is one aspect, deriving in part from the fact that the Internet is a network of mostly interoperable networks of varying robustness and resilience. But this is not a matter of design alone; the continuing evolution of ICT networks and systems – and of uses and users - means that old systems, code, devices and architectures will remain, interacting with their newer counterparts. Both opportunities and incentives for maintenance of this complexity are limited, and in some cases impossible. 5G networks will certainly need to deal with current vulnerabilities and at the same time to contribute to availability of more secure systems. Protection of data against destructive and insecure use and securing the utility and integrity of data depends on the ability of systems to recognise identities and protect against sniffing and access by those who should not have access and to detect and limit inappropriate use of data by those allowed access. IoT/CPS clearly has to address a wide range of vulnerabilities of varying criticality (to be considered). [section 1]

Secondly, we describe the socio-economic-political situation and its interaction with cybersecurity. It may be clear that specific actors may step up their efforts to reduce the risk of security breaches when vulnerabilities become their clear responsibilities. Again, there are clear specific aspects reflecting the three Picasso domains. 5G networks will greatly influence mobility and offer additional forms of connectivity with different security challenges than IP networks. With (Big) Data, specificities the heighten the stakes include: concepts like data ownership, governance and value; ; the increasing significance of the algorithms that operate on (and shape) data flows; and the growing tension with value of data "in the public interest" and value of data to individual actors. With regards to IoT/CPS, specific challenges arise from the gaps between the potential, intended and actual application of "things" and systems. Many current vulnerabilities relate to commercial competition based more on competing on 'features' and minimising time-to-market rather than enhancing "robustness of systems" - many people (customers and suppliers alike) still consider ICT devices as gadgets even as more and more aspects of their lives depend on their reliable and secure functioning; in any case, robustness, risk and resilience of such technologies and systems are still poorly understood. [section 2]

After that we focus on new developments likely to affect the security and vulnerability of ICT systems and the information ecosystem as a whole. We find that new legislation raises the stakes for businesses and seems to seek to provide incentives for improved security by raising the severity of penalties for system failures (i.e. accountability of suppliers of ICT tools and services). But we also see further globalisation of ICT driven markets and value chains, which could open up possibilities for new forms of standards setting and certification. [This will be the focus of our next policy paper]. This section goes deeper in the three specific PICASSO technological areas, drawing on the work of the PICASSO expert groups and we will provide a starting point to collect their further input to identifying connections between policy and R&I collaboration. [section 3]

Building on these, Section 4 explores possible ways to address the challenges that cybersecurity policies pose to collaborative R&I and to improve the impacts of collaborative R&I in the PICASSO domains on cybersecurity policy. Roughly, these can be divided between ways to make the best out of what we have by reducing dependencies on insecure infrastructures and mitigation and reduction the incidence and severity of cybersecurity failures on one side and redesigning the infrastructures on which we currently rely and devising new ways of using them that are relatively immune to existing and emerging cybersecurity threats. We discuss both approaches (mitigation and adaptation), what they would entail, and how they could practically be assessed and ultimately implemented. [section 4]

In conclusion, we see many opportunities for collaboration in this field, which concerns truly global issues and global technology development and applications. We are inviting proposals for specific conclusions lead to possible opportunities for EU US ICT collaboration, particularly aimed at the domains of 5G networks; Big Data; and the IoT/CPS.

PROPOSED WEBINAR AGENDA

PICASSO will organise a webinar on Cybersecurity on 16 May 2017, 15:00 UTC. Participation to the Webinar is free, and people are requested to register beforehand. Webinar registered participants will have received this draft paper in preparation of the webinar, and have been asked to read this and advance any questions coming up prior to the webinar thus allowing a further preparation of the agenda on topics that have been raised by multiple participants.

1- Welcome and purpose of the call. PICASSO, its focus, and the specific aims of this call
Maarten Botterman, Chairman of the PICASSO Policy Expert Group
2- Introduction to EU-US Cybersecurity technology issues relating to ICT development;
Dr. David Farber, Carnegie Mellon University, IEEE fellow, ACM fellow
3- Introduction to EU-US Cybersecurity policy issues relating to ICT development;
Dr. Jonathan Cave, GNKS Consult and University of Warwick

Participatory discussion: current status and expected development in EU and US

4- Introducing the three domains 5G; Big Data; IoT/CPS.
Dr.Gerhard Fettweis, Chairman of the PICASSO 5G Networks Expert Group (tbc)
Dr.Nikos Saris, Chairman of the PICASSO Big Data Expert Group (tbc)
Dr. Sebastian Engell, Chairman of the PICASSO IoT/CPS Expert Group (tbc)
Dr. Tariq Samad, Co-Chairman of the PICASSO IoT/CPS Expert Group (tbc)

Introduction and participatory discussion:

a. Focus per domain
b. Cybersecurity issues relevant for each domain (Taxonomy of privacy sensitivity in the domain)
c. How this affects the domain and EU-US collaboration in this domain

5- Preliminary conclusions

All introductions will be 10 minutes max followed by discussion. The total webinar will last for 90 minutes max and will be interactive. Focus is on Cybersecurity aspects relevant for the PICASSO domains.

PLEASE JOIN THE PICASSO Webinar on Cybersecurity on 16 May 2017 , 15:00 UTC