A platform to promote policy debate and provide opinions and recommendations for ICT cooperation between Europe and North America

ICT DIALOGUES

DISCOVERY

Co-funded by the Horizon 2020 Framework Programme of the European Union

Working Group - Funding Mechanisms

- What funding instruments should be used to promote European – North-American(ICT) research collaboration?
- Best practices, what works and what does not work?
- Do we have appropriate Funding mechanisms today?

- White paper on funding mechanisms is in the making
- Finished in Q1-2017
- Working group with representatives from US, Canada and Europe
- If anyone is interested in contributing contact me

Co-funded by the Horizon 2020 Framework Programme of the European Union

Working Group - Cybersecurity

- Experts representing and connecting to a broad network of researchers and innovators involved in projects, initiatives and platforms related to cybersecurity;
- Balanced membership between the EU, US and Canada experts;
- Main instrument for DISCOVERY to ensure high quality debate and engagement in relation to international collaboration in this vitally important topic;
- Best practices, what works and what does not work, why INCO is needed?
- Identification of cybersecurity technological gaps and issues currently existing in Europe, US and North America pointing out the common challenges and threats experienced by research and industry bodies (in EU, US, Canada);

Co-funded by the Horizon 2020 Framework Programme of the European Union

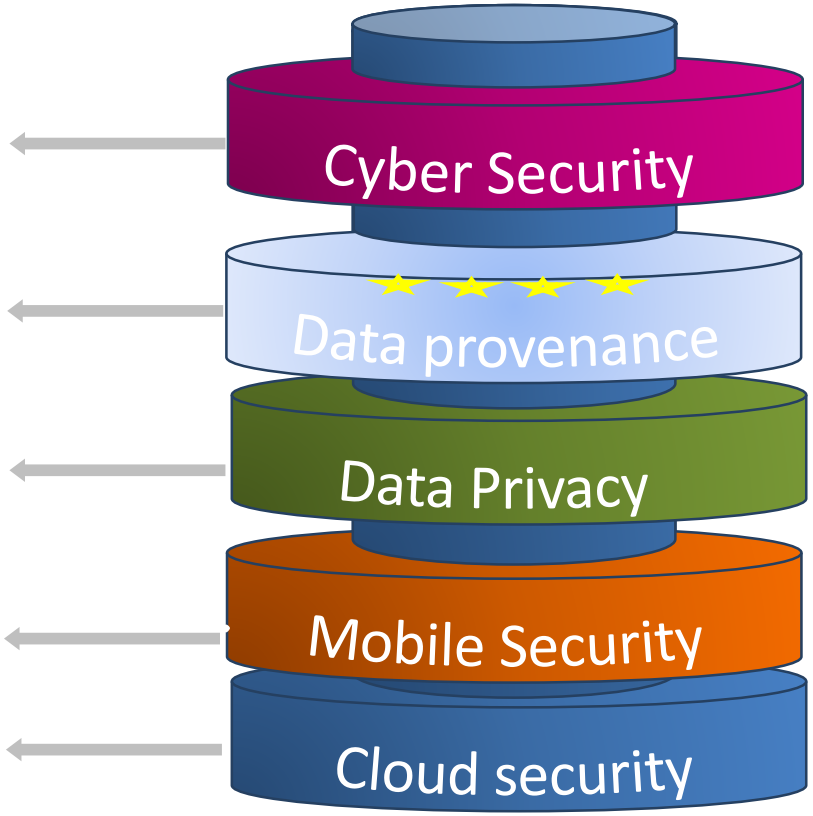
Working Group - Cybersecurity

- Furnish suitable recommendations to address and target these identified challenges, gaps and issues. Working together with the DISCOVERY consortium, the Cybersecurity Working Group will discuss open issues regarding data security, trust and privacy of such systems;
- Position paper (draft 1) already online;
- Members part of this afternoon session – full list at http://discoveryproject.eu/transatlantic-ict-forum/cybersecurity/
- Membership is still open - If anyone is interested in contributing, contact us

Co-funded by the Horizon 2020 Framework Programme of the European Union

EU-North America cybersecurity topics

From position paper – draft 1.



- International data exchg. Architecture for cyber-security
- Fight against cyber crime, malware
- Align policies and joint exercises
- Cryptography

- Affirming source/birth of data
- **Audit trails for sectors (e.g. Gov't.)**
- Standards on provenance models

- Smart technologies and privacy
- Future internet techs. and privacy
- Social networking and privacy
- Increase uptake of Privacy by Design and PIA

- Balance between strong security tools and efficiency and effectiveness - Security with flexibility
- Security that affects every day citizens
- Empowering the citizens to take charge of their mobile security.

- Including Cloud Security as a Service to imrove security and privacy
- Risk models
- Uniform uptake of Cloud solutions
- Security of data centres.

Co-funded by the Horizon 2020 Framework Programme of the European Union

Cybersecurity Panel Members

- Jacques Bus, Secretary General, Digital Enlightenment Forum
- Evangelos Markatos, Head of the Distributed Computing Systems Laboratory, Foundation for Research and Technology (FORTH), Greece and member of EU-US project PROTASIS.
- Fabio Martinelli, Senior researcher and leader of the cyber security project at IIT-CNR, Italy, NIS Platform co-chair of WG3, cPPP co-chair of SRIA ECSO Working Group
- Dan Caprio, Co-Founder, Chairman, The Providence Group, US
- Menouer Boubekeur, Strategic Business Development, PI Cyber Physical Systems, United Technologies Research Center, Ireland
- Tina Höfinghoff, CEO MUC Summit GmbH, Germany (apologies)
- Nina Olesen, Policy Manager, European Cyber Security Organisation (ECSO) (apologies)
- Crister E. Hammerlund, Unit H1, Trust and Security, DG CONNECT.

Co-funded by the Horizon 2020 Framework Programme of the European Union

Working Group - Cybersecurity

1. Research involving the wider scope of Cybersecurity
   - Convergence of physical and cyber worlds e.g. IoT
   - Appropriate coordinated regulations
   - International Data Exchange for cybersecurity
   - Dealing with threats, attackers and hacktivists
   - E-governance, information sharing, sharing of best practices, surveillance and analysis, joint exercises in cybersecurity and training, and joint research activities
   - Cybercrime (virus in email, botnets, Trojan in webpage, fraud in ecommerce, e-robbery in e-banking transaction, identity theft in credit card payment, …).
   - Cyber-terrorism: Terrorism on physical telecom infrastructures (fixed or wireless telecommunication network operations)
   - CERTs (Computer Emergency Response Team) recognised as premier references
   - Protection against malware
   - Cryptography.

Co-funded by the Horizon 2020 Framework Programme of the European Union

Working Group - Cybersecurity

2. Future Internet (FI) Data and Information provenance (trust of birth or source of data/information)
   - Scientific Domains: Scientists deal with greater heterogeneity in data and metadata
   - Virtual organizations: Workflows, warehouse environments, where lineage information is used to trace the data in the warehouse view back to the source from which it was generated.
   - Governmental Domains within the social inclusion policies, E.g. Voting system, taxing system
   - Data Quality: Use of lineage to estimate data quality and data reliability
   - Audit Trail: Tracing of the audit trail of data, determine resource usage and errors in data generation
   - Replication Recipes: Allow repetition of data derivation, help maintain its currency and re-do replication
   - Attribution: The pedigree can establish the copyright and ownership of data
   - Informational lineage: Use of lineage to query metadata for data discovery.
   - Applications of collecting and modelling provenance from heterogeneous applications and data sources
   - Standardization of provenance models, services, and representations, provenance management architectures and techniques.

Co-funded by the Horizon 2020 Framework Programme of the European Union

Working Group - Cybersecurity

3. Future Internet (FI) Data and Information privacy
   - Smart technologies and privacy
   - Privacy by design principles, including Privacy Impact Assessment (PIA)
   - Future Internet technologies and privacy
   - Universality of trust and privacy
   - Standardisation: EU's PRIPARE project and expert group in PICASSO
   - Anonymity and Pseudonymity.

Co-funded by the Horizon 2020 Framework Programme of the European Union

Working Group - Cybersecurity

4. Mobile Security
   - Mobile connectivity that accommodates the heterogeneity and failure-proneness of both devices and network to gel with issues such as broadband and sparse coverage areas in rural settings.
   - Balance between strong security tools and efficiency and effectiveness - Security with flexibility
   - Security that affects every day citizens
   - Empowering the citizens to take charge of their security.

Co-funded by the Horizon 2020 Framework Programme of the European Union

Working Group - Cybersecurity

5. Cloud security (including Security as a Service)
   - Risk models: The different nature of business environments and political landscapes between EU and other countries require a fresh look into the risks of using delocalised processing and storage of data and information.
   - Uniform uptake of Cloud solutions: The uptake of cloud computing solutions should be analysed between countries
   - Security of data centres: The evolution of data centres remains a key driver of Cloud computing ecosystems
   - Use of the cloud platforms as an innovative technology to improve security and privacy.

Co-funded by the Horizon 2020 Framework Programme of the European Union