A Look at the EU Support of Research in Cybersecurity

"Incident management and countering targeted cyber-physical attacks in distributed large-scale critical systems (IM&CTCPA 2016)"

International scientific school

Alexey Kirichenko, November 2, St. Petersburg

F-Secure

Cybersecurity Lives Here

F-Secure: Brief Intro

- Founded in 1988
- Headquartered in Helsinki
- Around 1000 employees and 25 offices, including Oulu (Finland), Kuala-Lumpur (Malaysia), Poznan (Poland), St. Petersburg (Russia), San Jose (US), Copenhagen (Denmark)
- Global leader in providing security as a service through telecommunication operators: over 200 Internet Service Provider and Mobile Network Operator partners in more than 40 countries.
- On the way of transforming from an end-point antivirus company to a broader provider of cyber security products and services.

Our Products & Services

- F-Secure SAFE and Internet Security
- F-Secure Freedome
- F-Secure SENSE
- Protection Service for Businesses and Client Security
- Rapid Detection Service
- F-Secure Radar
- F-Secure Software Updater

Research Collaboration

- Finnish national research collaboration projects:
  - Cyber Trust
  - Cloud Security Services
  - Data to Intelligence
- A partner in several ITEA and Celtic+ projects and in EIT Digital
- H2020 Scalable and Secure Infrastructures for Cloud Operations (SSICLOPS)
- H2020 Constructing an Alliance for Value-driven Cyber Security (CANVAS)
- Founding member in the just-formed European Cyber Security Organization (ECSO – cPPP)

Changes in Finland and Denmark

- Euroscientist.com: Research and education budgets in shambles in Denmark and Finland.
- They are among the few nations in Europe that have reached the target to allocate 3% of their countries' GDP to research and development, but the newly formed centre-right governments are adopting radical new policies.
- Denmark: reduce the budget for research by about DKK1.4 billion (€190 million) to DKK20.6 (€2.8) billion, a cut of about 6.3 % compared to 2015.
- In Finland, a governmental proposal suggests a cut of about 9% of the overall research budget, representing €140 million in 2016 compared to 2015.
- The same applies to the budgets for higher education.
- Elsewhere in Europe, right-wing parties are also increasingly gaining support…
- "… research should be seen as a way to emerge from economic difficulties not as a source of savings in austerity regimes."

EU Funding Forms and Ways

R&I Funding Instruments in Europe

- Horizon 2020
- European Research Council (ERC) grants https://erc.europa.eu/funding-and-grants
- EIT Digital: a leading European digital innovation and entrepreneurial education organisation driving Europe’s digital transformation. Delivers breakthrough digital innovations to the market and breeds entrepreneurial talent for economic growth and improved quality of life in Europe. It does this by mobilising a pan-European ecosystem of over 130 top European corporations, SMEs, start-ups, universities and research institutes, a Knowledge and Innovation Community of the European Institute of Innovation and Technology.

R&I Funding Instruments in Europe: EUREKA

- EUREKA is an intergovernmental network launched in 1985, to support market-oriented R&D and innovation projects by industry, research centres and universities across all technological sectors. Offers project partners rapid access to skills and expertise across Europe and national public and private funding schemes. Focus is on R&D projects with a good business plan.
- Celtic-plus: the Telecommunication and ICT Cluster under the umbrella of EUREKA, focuses on telecommunication and ICT connecting people and businesses in a secure way. Key topics: network capacity, optics, satellite, mobility, security, robustness, energy efficiency, 5G, Smart Cities, Smart Homes, digital enterprises, e-health, big data, Internet of Things, privacy, identity and public safety. Industry-driven approach. Includes flagship projects with significant impacts.
  https://www.celticplus.eu/vision-and-mission/
- ITEA: EUREKA Cluster programme supporting innovative, industry-driven, pre-competitive R&D projects in the area of Software-intensive Systems & Services (SiSS). SiSS are a key driver of innovation in Europe's most competitive industries, such as automotive, communications, healthcare and aerospace.
  https://itea3.org/about-itea.html

Digitising European Industry

- https://ec.europa.eu/digital-single-market/en/digitising-european-industry
- "Digitising European Industry - Reaping the full benefits of a Digital Single Market" initiative, adopted by the European Commission in April 2016.
- The overall objective of the DEI initiative is to ensure that any industry in Europe can fully benefit from digital innovations.
- Digital Innovation Hubs; Public-Private Partnerships;
  Industrial Platforms and large scale pilots; Skills and training;
  Regulatory framework; Internet of Things; European Cloud Initiative; Standards;
  eGovermment Action plan
- Financing: Overall, today's plans should mobilise up to €50 billion of public and private investments in support of the digitisation of industry.

EU Initiatives

- The European Cloud Initiative https://ec.europa.eu/digital-single-market/en/european-cloud-initiative
- Advancing the Internet of Things in Europe https://ec.europa.eu/digital-single-market/en/news/staff-working-document-advancing-internet-things-europe
- Public Private Partnerships https://ec.europa.eu/digital-single-market/en/public-private-partnerships

Horizon 2020

- Horizon 2020 is the biggest EU Research and Innovation programme ever with nearly €80 billion of funding available over 7 years (2014 to 2020)
- Horizon 2020 is the financial instrument implementing the Innovation Union, a Europe 2020 flagship initiative aimed at securing Europe's global competitiveness.
- The Horizon 2020 work programme is complemented by the separate work programmes for the European Research Council, Euratom, the Joint Research Centre and the Strategic Innovation Agenda for the European Institute of Innovation and technology (EIT).

H2020 Sections

- Excellent Science: European Research Council, Future and Emerging Technologies, Marie Skłodowska-Curie actions, Research Infrastructures, including e-Infrastructures
- Industrial Leadership: Nanotechnologies, Advanced Materials, Advanced Manufacturing and Processing, and Biotechnology; Information and Communication Technologies; Space.
- Societal Challenges:
  - Health, Demographic Change and Wellbeing;
  - Food Security, Sustainable Agriculture and Forestry, Marine, Maritime and Inland Water Research and the Bioeconomy;
  - Secure, Clean and Efficient Energy;
  - Smart, Green and Integrated Transport;
  - Climate Action, Environment, Resource Efficiency and Raw Materials;
  - Europe in a changing world - Inclusive, innovative and reflective societies;
  - Secure societies – Protecting freedom and security of Europe and its citizens (this includes enhanced cyber-security)

Digital Security

- Until the end of 2013: FP7. From 2014 onwards: H2020, in two streams: Leadership in enabling and industrial technologies (LEIT) and Societal Challenges: in particular Societal Challenge 7, "Secure societies – Protecting freedom and security of Europe and its citizens"
- Digital Security is a multi-faceted issue involving critical economic and civilian stakes, cybercrime, online privacy and the protection of fundamental rights. Research in this area addresses security, trust and privacy coherently from all perspectives (technological, economic, legal, social).
- Research priorities address current ICT security challenges, like:
    - trustworthy network and service infrastructures
    - user-centric identity and privacy management and technologies for secure software development
    - trusted computing
    - cryptology
    - advanced biometrics

Projects in Digital Security: Recent Past

- Around 50 projects, staring from 2010 up to now
- ~ EUR 190M of the EC contribution, roughly over the period of 3.5 years
- Project types:
  - Research and Innovation (37)
  - Coordination and Support (10)
  - Pilots, collaboration

Key Domains

- Program analysis tools, formal methods, model checking, pen testing
- Fighting botnets, threat and vulnerability data gathering and analysis
- Decision support system, risk based approach and analysis engines, continuous and predictive cyber security monitoring and response capability
- Visual analytics technologies for the identification and prediction of very complex patterns of abnormal behavior
- Protecting smart mobile devices, offloading execution of security applications into a programmable device at the edge of the network
- Web application security

Key Domains

- Security of Cloud services, data management in the cloud, SLAs
- Certification of security properties of IaaS, PaaS, and SaaS services in the cloud
- Platform security, security engineering process, integrity checking technologies, biometrics
- Security testing and security assessment
- Privacy-preserving attribute-based authentication and use of unique identifiers
- eAuthentication and eAuthorization, federation
- Critical system construction and certification, MILS
- Policy modeling, validation
- Sensor networks, secure integration of sensor networks into large scale industrial environments
- Cognitive model of user trust perception

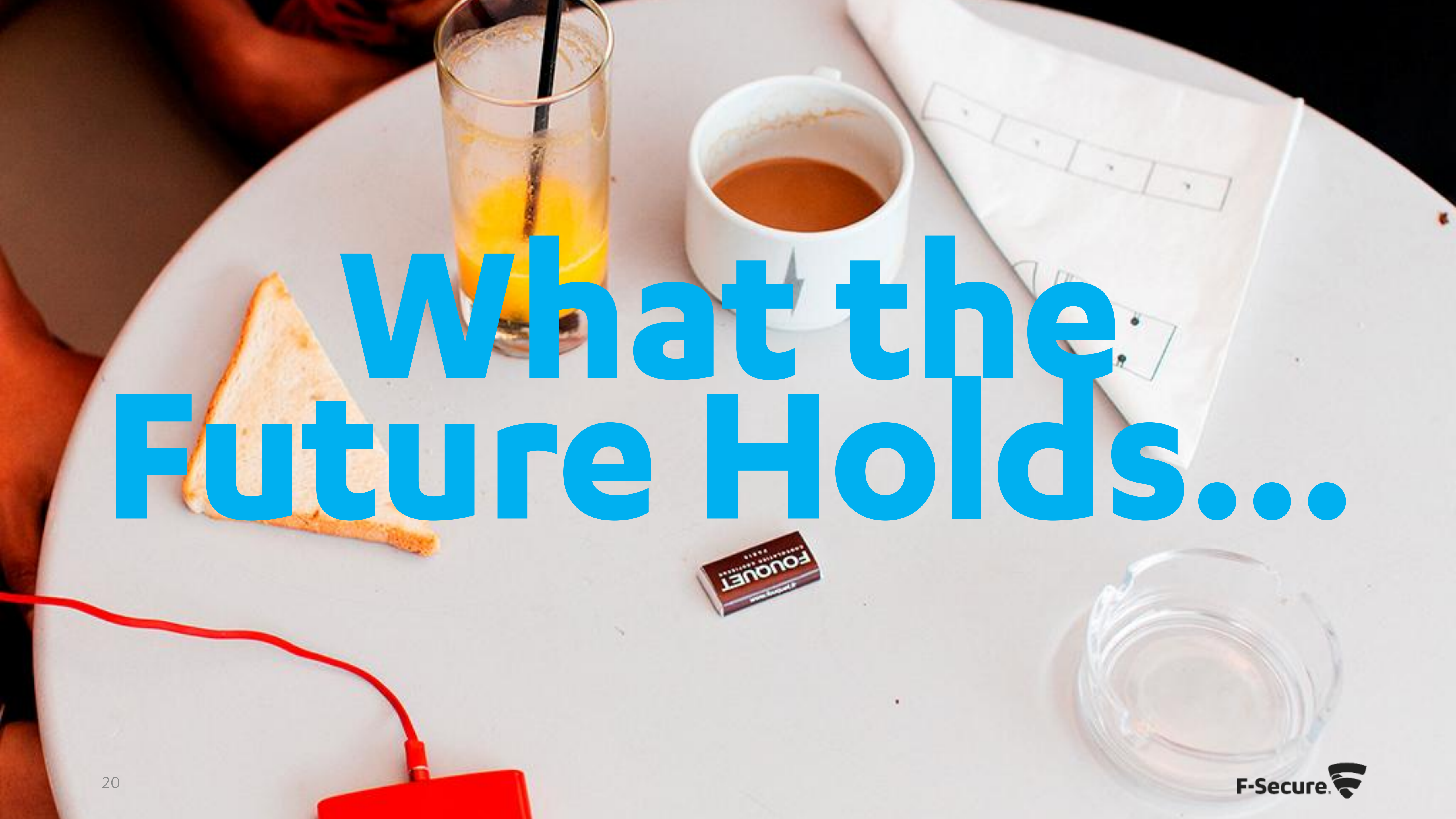
Investments

These are rough estimates, as many projects contributed to multiple domains.

- "Clouds": EUR 34M
- Situational awareness, risk analysis, response: EUR 28M
- eAuthentication and eAuthorization, identity management, federation: EUR 22M
- Security assessment, policy modeling and validation: EUR 20M
- Platform security: EUR 15M

How the Countries Fared

- DE: 44.6M; FR: 22M
- IT: 17.7M; UK: 13.8M; ESP: 15.2M
- AT: 8.3M; BE: 9.1M; NL: 10.1M; NOR: 9.32M; SUI: 8.4M
- GRE: 4.9M; SWE: 3M; PT: 2.9M; DK: 4.8M; IRE: 2.9M
- HUN: 1.33M; FIN: 1.29M; LUX: 1M; RO: 1M; EST: 1.4M
- SLO, BUL, CRO, CZE, POL, CYP: tiny
- Turkey, South Africa; China: tiny
- Russia: 0.9M (SPIIRAS)
- Israel: 3M



What the Future Holds…

EU Public-Private Partnerships

- The EU research framework programme – Horizon 2020 – may be implemented through public-private partnerships (PPPs) in the case of research and innovation activities of strategic importance to the Union's competitiveness and industrial leadership, or to address specific societal challenges.
- Contractual PPPs follow the H2020 rules and procedures, with industry providing key advice on research priorities. (JTIs are run as Joint Undertakings.) The contractual arrangement forming the basis for each cPPP is signed by the EC and representatives of the respective industry grouping. It specifies the partnership's objectives, commitments, key performance indicators, and expected outputs.

cPPP’s

- https://ec.europa.eu/digital-single-market/en/public-private-partnerships
  - provide a legal structure to pool resources and to gather critical mass
  - make research and innovation funding across the EU more efficient by sharing financial, human and infrastructure resources
  - can provide the right framework for international companies to anchor their research and innovation investments in Europe
- Cybersecurity; Photonics; High Performance Computing; Robotics; Future Internet; 5G; ECSEL; Factories of the Future.

Cybersecurity cPPP

- The EC signed agreement with industry on cybersecurity: cPPP (July 5)
  - ECSO established to lead the cPPP implementation
- The EC will invest €450 million in this partnership, under its research and innovation program Horizon 2020 for the 2017-2020 calls (4 years).
- Main strategic objectives:
  - Protection from cyber threats of the growth of the European Digital Single Market
  - Creation of a strong European-based offering and an equal level playing field for trustworthy and privacy aware solutions
  - Growth and presence of European cybersecurity industry in the global market
  - Elaboration and indication of the addressed minimum level of security, with a workable guideline for supportive policy activities such as certification and labelling

Industrial Cybersecurity Challenges in Europe

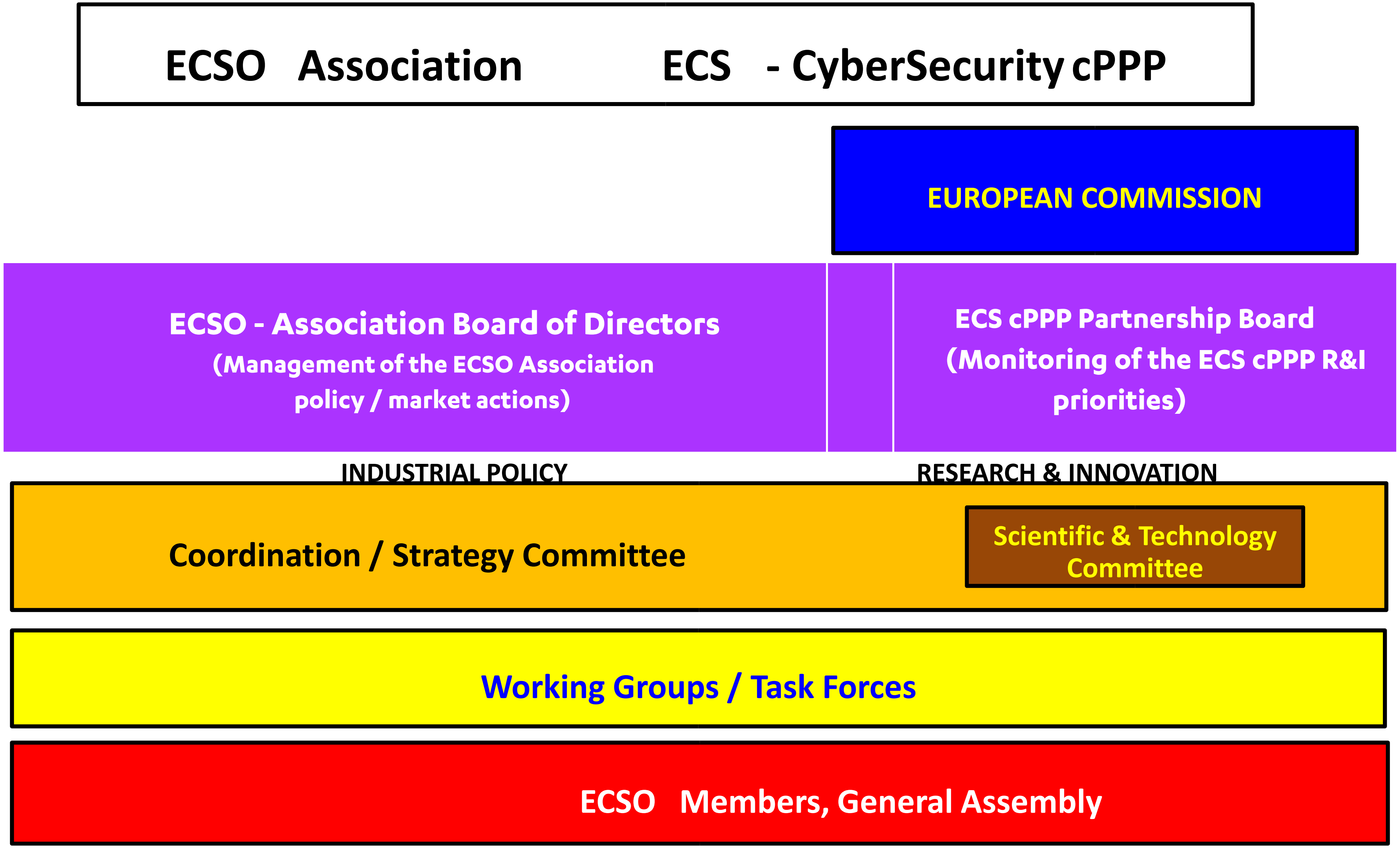
- Global cybersecurity and ICT market dominated by global suppliers from North America
  - Innovation led by imported ICT products
  - Financial. Weak entrepreneurial culture, lack of venture capital.
- Innovation: strong in Europe but not always properly funded due to a lack of a consistent transnational approach. Results of Research and Innovation are hardly reaching the market. There is still a lack of strategy in European research.
- Imperfect coordination, a lot of disconnected efforts addressing the same challenges.

What CyberSecurity cPPP Means in Practice

- Forming agenda for H2020 calls in Cyber Security
- Priorities for the EU Research and Innovation agenda in Cyber Security and how the funding is distributed for supporting it
- Possibly establishing and coordinating other initiatives in the area
- Vehicle for communicating with the EC
- 70M€ will be used in the 2017 calls. The remaining 380M€ of EC funding should be distributed progressively: 110 M€ in 2018, 130M€ in 2019, 140M€ in 2020.

EUROPEAN CYBERSECURITY ORGANISATION (ECSO)

- Proposing in cooperation with the EC a Strategic Research and Innovation Agenda (SRIA) and its updates – the main role
- Priorities for development of European cybersecurity solutions and services and support their implementation within the H2020
- Definition and implementation of elements of a European cybersecurity industrial policy



ECSO Association

ECS - CyberSecurity cPPP

EUROPEAN COMMISSION

ECSO - Association Board of Directors
(Management of the ECSO Association policy / market actions)

ECS cPPP Partnership Board
(Monitoring of the ECS cPPP R&I priorities)

INDUSTRIAL POLICY

RESEARCH & INNOVATION

Coordination / Strategy Committee

Scientific & Technology Committee

Working Groups / Task Forces

ECSO Members, General Assembly

Proposed SRIA Priorities and EC cPPP Funding

While the domains are chosen (and not very surprising), the funding levels are under discussion and will likely change.

- Fostering assurance and security and privacy by design (20M)
- Identity, access and trust management (18M)
- Data protection, including encryption (34M)
- Protecting the ICT Infrastructure and enabling secure execution (78M): Cyber Threats Management, Network Security, System Security, Cloud Security, Trusted HW/EP security/mobile security
- Security services (28M): Auditing, compliance and certification, Risk Management, Managed security services, Security training

Assurance and Security and Privacy by Design

- Security / Privacy by Design
- Secure (programming) languages and frameworks
- Security validation
- Metrics
- Methods for development of functionally correct and error free security protocols and interfaces
- Combination of functional safety and security
- Methods for developing resilient systems out of potentially insecure components

IdM and Trust

- Usability of authentication
- Flexibility of authentication and authorization
- Partial identities
- Certificate and signature sustainability
- Scalability of authentication
- Interoperability of authentication
- Computational trust models
- Decentralized trust frameworks (blockchain/distributed ledger)
- Trust and big data
- Credential personalisation

Data Protection and Crypto

- Data protection techniques
- Privacy-aware Big Data analytics
- Secure data processing
- User empowerment
- Operations on encrypted data
- Provenance and quality of data
- Query privacy
- Big data secure storage

Protection of ICT Systems

- Secure network design, usage and management
- Control and intrusion prevention systems
- Secure integration
- Secure execution platforms
- Bring Your Own Device
- Security-supporting services
- Operating systems (OS) security
- SIEM

Cybersecurity Services

- Security-supporting services
- Practical Certification Schemes
- Methods to reduce and manage systems complexity
- Quantification of Risk
- Dynamic Risk assessment and management
- Cyber Insurance
- Security validation
- Down-scaling and Up-scaling

Upcoming Calls

Addressing Advanced Cyber Security Threats and Threat Actors

- http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/ds-07-2017.html
- Deadline: 24 August 2017 17:00:00
- A: Research and Innovation Actions –Situational Awareness
  a contribution from the EU between EUR 2M and 3M, TRL 3 - 5
- B: Innovation Actions – Simulation Environments, Training
  a contribution from the EU between EUR 4M and 5M, TRL 6 - 7

TRL means Technology Readiness Level, explained on the EC portal.

DS-07-2017: Situational Awareness

- Novel approaches for providing organisations the appropriate situational awareness in relation to cyber security threats allowing them to detect and quickly and effectively respond to sophisticated cyber-attacks
- Interdisciplinary research to counter threat actors and their methods
- Should also consider the need to collect necessary forensic information from attackers that can be used as evidence in court
- Should assess and address the impact to fundamental rights, data protection and privacy in particular, in the design and development of their solutions

DS-07-2017: Simulation Environments, Training

- Innovative simulation environments and training materials in order to adequately prepare those tasked with defending high-risk organisations to counter advanced cyber-attacks
- Tools for creating realistic cyber environments that fit the training objectives and tools for producing both benign and malicious system events that fit the training scenario
- Real-time student performance assessment, dynamic configuration and adaptation of exercise scope and difficulty
- Definition and creation of new scenarios and cyber threats in a cost and time-effective manner, and that better achieve the pedagogical objectives for a wide variety of student profiles
- Scenario building and simulation training to prepare organisations' response and decision making processes in relation obligations stemming from applicable legal frameworks or in the wider context of managing crises and emergency situations

Privacy, Data Protection, Digital Identities

- http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/ds-08-2017.html
- Deadline: 24 August 2017 17:00:00
- Innovation Actions
  A contribution from the EU between EUR 2M and 3M, TRL 6 – 7
- Privacy-enhancing Technologies
- General Data Protection Regulation in practice
- Secure digital identities
- For all strands, proposals should identify and address the societal and ethical dimensions of the strand they choose to cover taking into consideration the possibly divergent perspectives of pertinent stakeholders.

Prevention, detection, response and mitigation of the combination of physical and cyber threats to the critical infrastructure of Europe

- http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/cip-01-2016-2017.html
- Deadline: 24 August 2017 17:00:00
- Innovation Actions
  A contribution from the EU up to EUR 8M, TRL7
- Proposals should focus on one of the following critical infrastructures: Water Systems, Energy Infrastructure (power plants and distribution), Transport Infrastructure and means of transportation, Communication Infrastructure, Health Services, Financial Services

R&I on IoT integration and platforms

- http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/iot-03-2017.html
- Deadline: 25 April 2017 17:00:00
- Research and Innovation action
  A contribution from the EU between EUR 3M - 5M
- IoT security and privacy. Advanced concepts for end-to-end security in highly distributed, heterogeneous and dynamic IoT environments. Approaches must be holistic and include identification and authentication, data protection and prevention against cyber-attacks at the device and system levels.
- Enabling novel, advanced semi-autonomous IoT applications.
- Increase of IoT usability and user acceptance, notably through strengthened security and user control.

Thank You

alki@f-secure.com