ECSO

European Cyber Security Organisation

contractual PPP on cybersecurity

WG6 on Strategic Research and Innovation Agenda

Fabio Martinelli

National Research Council of Italy

ECSO-WG6 co-chair

Outline

- ECSO cPPP
- ECSO WG6 SRIA
- ECSO input to H2020 (WP 18-20)

ABOUT THE CYBERSECURITY cPPP

AIM

1. Foster cooperation between public and private actors at early stages of the research and innovation process in order to allow people in Europe to access innovative and trustworthy European solutions (ICT products, services and software). These solutions take into consideration fundamental rights, such as the right for privacy.

2. Stimulate cybersecurity industry, by helping align the demand and supply sectors to allow industry to elicit future requirements from end-users, as well as sectors that are important customers of cybersecurity solutions (e.g. energy, health, transport, finance).

3. Coordinate digital security industrial resources in Europe.

LINKING RESEARCH AND CYBERSECURITY INDUSTRIAL POLICY

1. The cPPP will focus on R&I, developing a SRIA (Strategic Research and Innovation Agenda).

2. The ECSO Association will tackle other industry policy aspects.

3. ECSO supports the development of the European cybersecurity industry.

ABOUT THE CYBERSECURITY cPPP

BUDGET:

1. The EC will invest up to €450 million in this partnership, under its research and innovation programme Horizon 2020 for the 2017-2020 calls (4 years).
2. Cybersecurity market players are expected to invest €1350 million three times more (€1350 million: leverage factor = 3) for a total of €1800 million

REFERENCE DOCUMENTS

1. Industry proposal
2. Strategic Research and Innovation Agenda (SRIA) proposal

INDUSTRY PROPOSAL

Identifies industrial operational and strategic objectives

1. Protection of critical infrastructures from cyber threats.
2. Use of massive data collection to increase overall security.
3. Increased European digital autonomy.
4. Security and trust of the whole supply chain
5. Investments in areas where Europe has a clear leadership.
6. Leveraging upon the potential of SMEs.
7. Increase competitiveness.

ECSO MEMBERS

ECSO has been established during June 2016 and on July 5th the ECS-cPPP has been approved by the European Parliament.

218 organisations having formally requested membership … from 27 countries and counting… divided in categories (each represented at the Board of Directors).

- Associations : 18
- Large companies: 55
- Public Administrations: 14 (UK, ES, IT, FR, DE, SK, EE, FI, NO, CY, PL, NL, CZ, AT)
- Regional clusters; 2
- RTO/Universities: 51
- SMEs: 40
- Users/Operators (users are also in large supplier companies): 8

AUSTRIA	6	ITALY	30
BELGIUM	4	LATVIA	1
BE - EU ASS	8	LUXEMBOURG	3
CYPRUS	4	NORWAY	4
CZECH REP.	1	POLAND	6
DENMARK	2	PORTUGAL	5
ESTONIA	4	ROMANIA	2
FINLAND	7	SLOVAKIA	2
FRANCE	21	SPAIN	29
GERMANY	16	SWEDEN	1
GREECE	2	SWITZERLAND	3
HUNGARY	1	THE NETHERLANDS	10
IRELAND	1	TURKEY	2
ISRAEL	2	UNITED KINGDOM	10

ECSO: A UNIQUE PPP ASSOCIATION

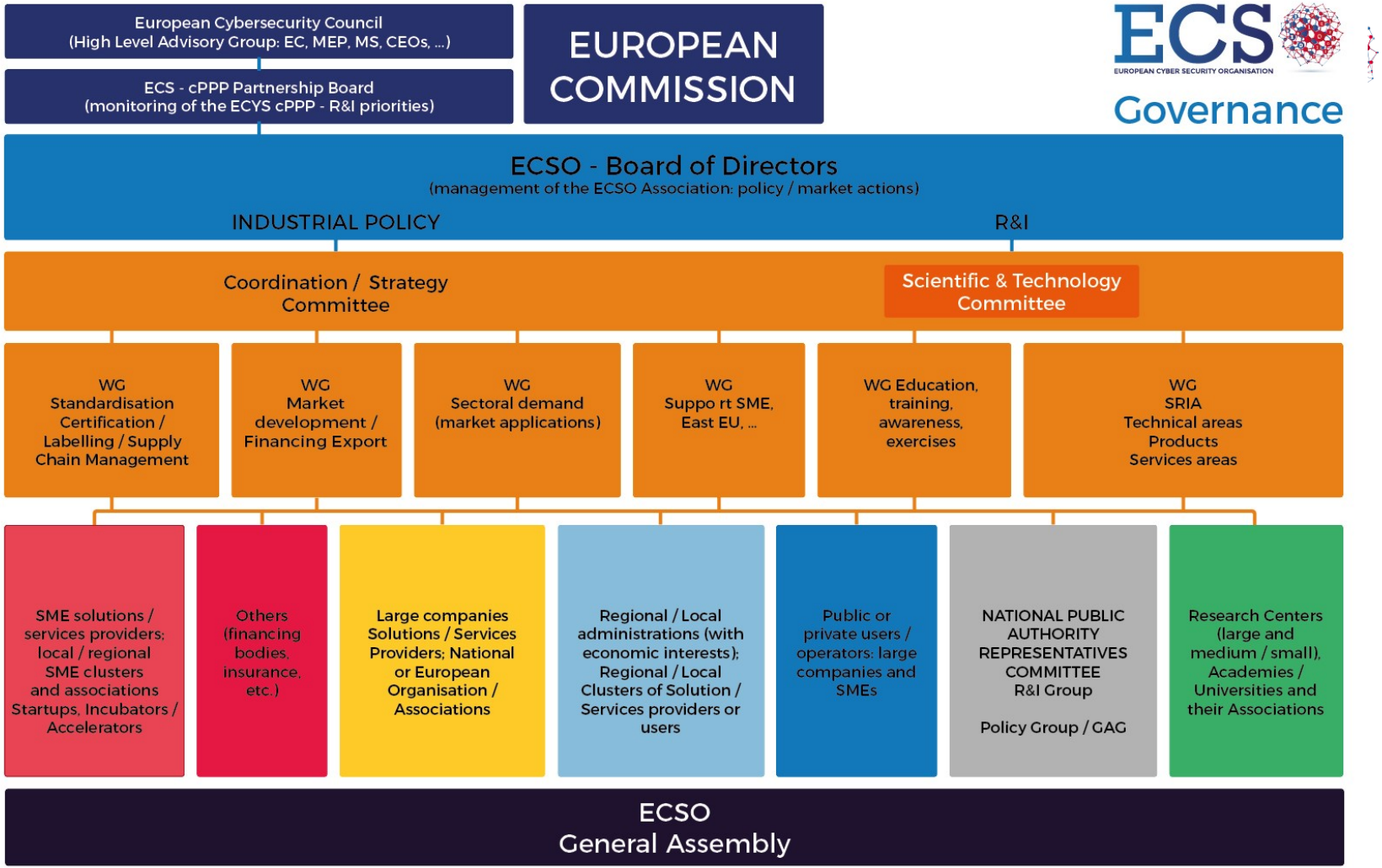
Security is a national prerogative.

➔ Stronger participation in ECSO of representatives from the national administrations, also at decision making level.

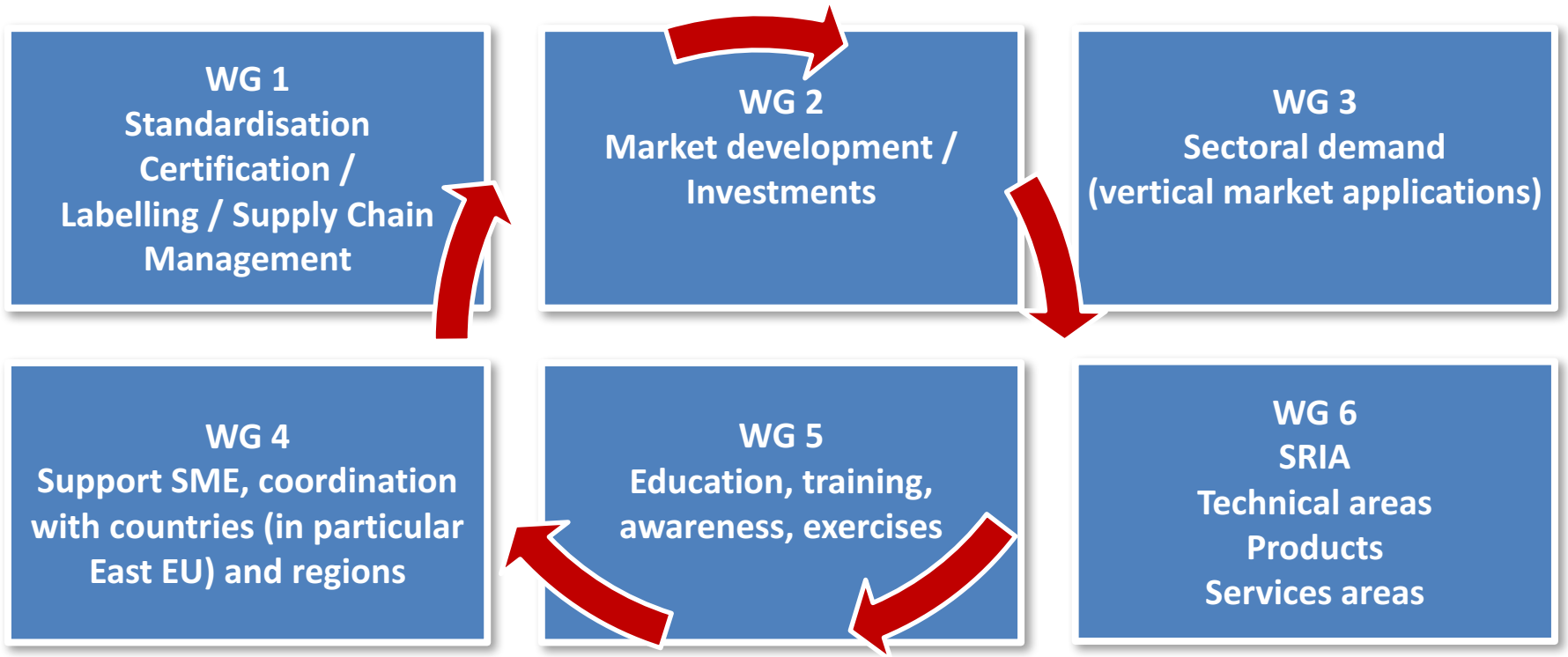
➔ Interest from national Public Administrations: Representatives to the two Programme Committees + Ministries (Interior, Economy, etc.) + Regulatory Bodies + Public users.

➔ Participation in Working Groups & Task Forces to bring a governmental perspective and operational needs from the public administrations.

NAPAC : A National Public Authority representatives Committee (NAPAC), instead of traditional "mirror groups".


European Cybersecurity Council
(High Level Advisory Group: EC, MEP, MS, CEOs, ...)
ECS - cPPP Partnership Board
(monitoring of the ECYS cPPP - R&I priorities)
EUROPEAN COMMISSION
ECS
EUROPEAN CYBER SECURITY ORGANISATION
Governance
ECSO - Board of Directors
(management of the ECSO Association: policy / market actions)
INDUSTRIAL POLICY
R&I
Coordination / Strategy Committee
Scientific & Technology Committee
WG Standardisation Certification / Labelling / Supply Chain Management
WG Market development / Financing Export
WG Sectoral demand (market applications)
WG Suppo rt SME, East EU, ...
WG Education, training, awareness, exercises
WG SRIA Technical areas Products Services areas
SME solutions / services providers; local / regional SME clusters and associations Startups, Incubators / Accelerators
Others (financing bodies, insurance, etc.)
Large companies Solutions / Services Providers; National or European Organisation / Associations
Regional / Local administrations (with economic interests); Regional / Local Clusters of Solution / Services providers or users
Public or private users / operators: large companies and SMEs
NATIONAL PUBLIC AUTHORITY REPRESENTATIVES COMMITTEE R&I Group
Policy Group / GAG
Research Centers (large and medium / small), Academies / Universities and their Associations
ECSO
General Assembly

WORKING GROUPS & TASK FORCES



Global overview of WGs activities

- **WG1 (standards / certification / label / trusted supply chain):** Initial informal suggestions were delivered to the European Commission with a plan of activities (continuous interactions at the technical level). State Of The Art (SOTA) document comprising an overview of existing cybersecurity standards and certification schemes relevant for the activities of WG1, and document analyzing the challenges and gaps relevant for the industrial sector. Next steps: start discussions on standards in preparation of the CEN/CENELEC workshop and cooperation with ETSI. Next full WG meeting March 14th-15th in Brussels. Contact: roberto.cascella@ecs-org.eu

- **WG2 (market/ funds/ cPPP monitoring):** WG to be started March 2017. Initial internal work on business models and funding programmes. Contact: danilo.delia@ecs-org.eu

- **WG3 (verticals: Industry 4.0; Energy; Transport; Finance / Bank; Public Admin / eGov; Health; Smart Cities):** Priority and objectives under detailed definition with users: state of the art deliverable (Del 1) setting out key requirements, issues, threats for each vertical, leading to enablement needs. Last WG meeting on February 9th. Meetings on specific sectors (e.g. WG 3.2 on energy & smart grids with DG ENER and DG CNECT on February 8th; WG 3.3 on transport on February 10th). Contact: nina.olesen@ecs-org.eu

- **WG4 (SMEs, Regions, East EU):** Meeting on Regional aspects with "Regions" (ECSO members and beyond) on March 7th. Discussion on other forms of support to SMEs other than R&D (e.g. EU regional funds). Next meeting on SMEs in Madrid on April 27th . Contact: danilo.delia@ecs-org.eu

- **WG5 (education, training, awareness, cyber ranges…):** One of the main priorities for MT and EE Presidency of the EU in 2017. Next meeting on March 17th in Tallinn for SWG 5.1 on ‘cyber range environments and technical exercises’. Contact: nina.olesen@ecs-org.eu

- **WG6 (SRIA):** Initial informal suggestions delivered to the European Commission and organisation of the priority topics identified by ECSO in the SRIA. Contacts with other PPPs and similar EU activities (5G, IoT, Big Data, Smart Cities, Photonics, Robotics, etc..) going to be started to coordinate objectives. Next WG meeting: March 9th in Brussels. Contact: roberto.cascella@ecs-org.eu

WG6 SRIA:
Technical areas, Products, Services areas

WG6 Chairs: Fabio Cocurullo (Leonardo), Volkmar Lotz (SAP), Fabio Martinelli (CNR)

Link to KPI (consistent with SRIA and Industry Proposal)

KPI 8 - PRIVACY & SECURITY BY DESIGN: Development and implementation of European approaches for cybersecurity, trust and privacy by design.

KPI 12 - cPPP IMPLEMENTATION MONITORING: Efficiency, openness and transparency of the cybersecurity cPPP implementation process.

Link to EU policies

Activities should be coordinated with the future activities envisaged by the E. Commission as announced in its Communication "Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry"

Objectives

O6.1: Coordination of results and expectations from EC R&I projects

O6.2: Coordination of cybersecurity activities across cPPPs and EIT

O6.3: Support cPPP implementation and H2020 cybersecurity projects

O6.4: Detailed suggestions for the WorkProgramme 2018 - 2020 using an updated and focussed SRIA

Initial WG6 SRIA: Segmentation

SWG 6.1: Ecosystem (chairs: H. Debar (IMT), J. Lopez (UMA), V. Pevtschin (ENG))

- **6.1.1** Link across R&I projects
- **6.1.2** Link with other cPPP / EC initiatives (5G, Cloud, IoT, Big Data, EIT etc.)

SWG 6.2: Vertical application domains (chairs: A. Fourati (EDF), Mari Kert (Guardtime))

- **6.2.1** Energy, including smart grids
- **6.2.2** Transport
- **6.2.3** Finance
- **6.2.4** Healthcare
- **6.2.5** Smart & Secure Cities
- **6.2.6** Public Services / eGovernment
- **6.2.7** Industrial Critical Systems / Industry 4.0

SWG 6.3: Trustworthy transversal infrastructures (chairs: A. Ayerbe (Tecnalia), P. Kearney (BT))

- **6.3.1** Digital citizenships (including identity management)
- **6.3.2** Risk management for managing SOC, increasing cyber risk preparedness plans for NIS etc.
- **6.3.3** Information sharing and analytics for CERTs and ISACs (includes possibly trusted SIEM, cyber intelligence)
- **6.3.4** Secure Networks and ICT (Secure and trusted Routers, Secure and Trusted Network IDS, Secure Integration, Open source OS).

SWG 6.4: Technical priority areas (chairs: F. Kirchner (CEA), E. Markatos (FORTH), P.H. Meland (SINTEF))

- **6.4.1** Assurance / risk management and security / privacy by design
- **6.4.2** Identity, access and trust management (including Identity and Access Management, Trust Management)
- **6.4.3** Data security
- **6.4.4** Protecting the ICT Infrastructure (including Cyber Threats Management, Network Security, System Security, Cloud Security, Trusted hardware/ end point security/ mobile security)
- **6.4.5** Security services

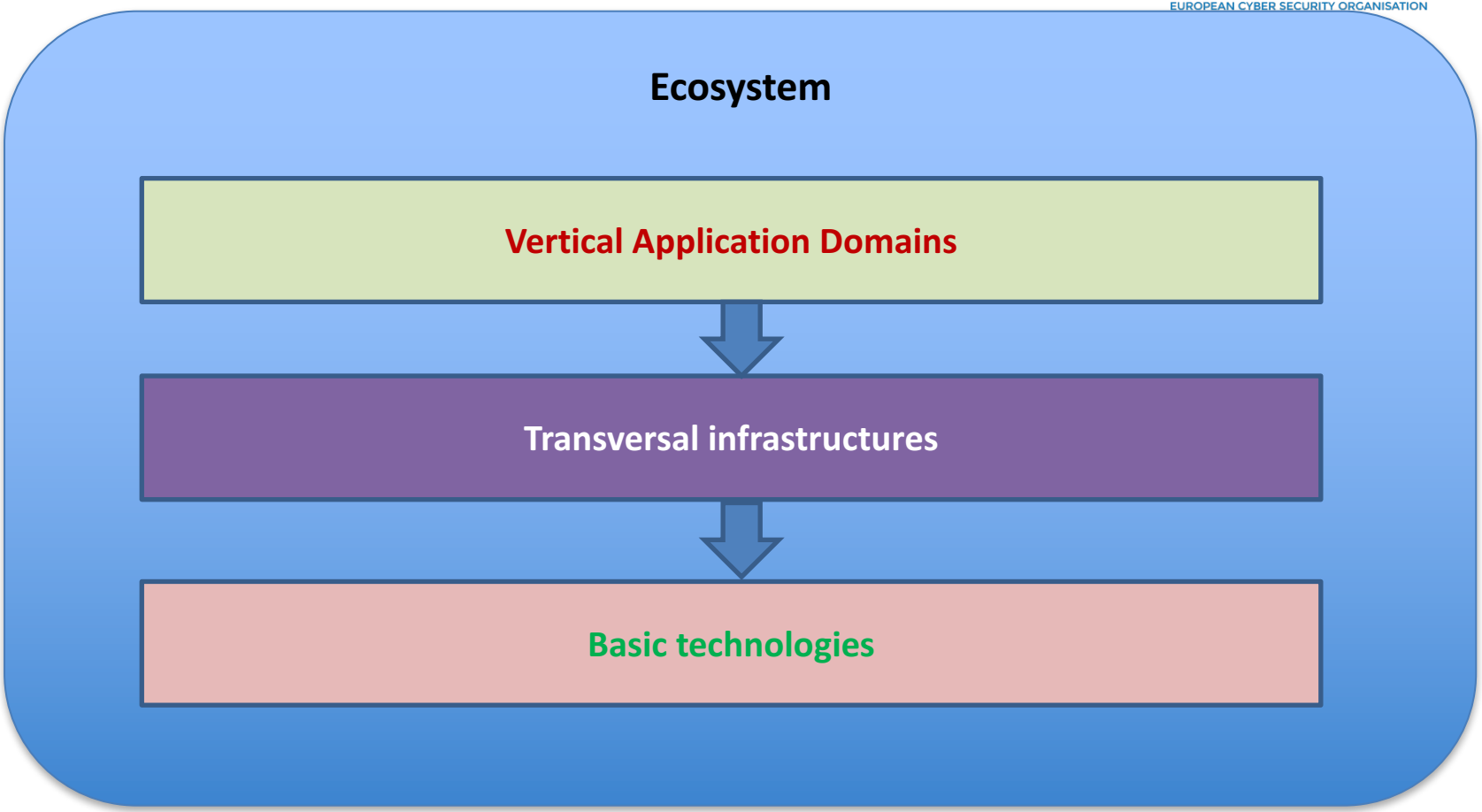
ECSO WG6 SRIA – Activities

- Using the cPPP SRIA v1.0 and industry proposal as initial guidelines
- WG6: 140 ECSO members, almost 250 experts
- Two initial WG6 meetings in Brussels (Sept. 12 and 14 2016): more than 100 people (from many sectors)
- Brainstorming groups, supported by facilitators/editors (according to the WG segmentation in sub WG)
- Collection of material and initial synthesis in a first draft: work done in parallel by the editors with several contributors per subWGs with 2 synchro conf call per week
- Distribution of the various major versions of the document to all SRIA WG members (in particular v. 1.13 with initial budget distribution)
- First draft commented and finalised on Oct. 3 (in less than 3 weeks). Presentation to the partnership Board Oct. 6 and ECSO Board Oct. 7: feedback and update, following PB and ECSO Board comments
- Presentation at **preparatory PC meeting on Oct 20th**: feedback for improvement
- Formal (ECSO approved) reccomendations sent to EC after the ECSO Board on Dec 15th
- Cooperation with the Commission to draft the WP
- Further improvements on the recommendations in January onwards and consolidated in the WG6 meeting in March 9th.
- Presentation to the Program Comittees of ICT/LEIT
- Cooperation with other WG (as WG3) for sectorial activities
- Cooperation with external organizations cPPPs
- Monitoring activities for KPIs
- Starting discussion for new vision document for ECSO WG6 SRIA (ready to FP9?)

Approach

- **Consider previous and ongoing EC projects** to plan future developments (analysis initiated: see next slide)
- To be done: **Work with other PPPs** to align goals and activities so as to ensure synergies and avoid duplications (integration of cybersecurity requirements and needs)
- Allow funding of basic and disruptive research, but **focus resources on security and competitiveness**: even with 380M€ we cannot cover all topics!
- The **cPPP is industry driven**: all stakeholders should concentrate efforts on security and economic sectors relevant to Europe.
- Main **demonstrators would be started asap using available technologies** also from previous projects. Further results from envisaged IA / RIA projects should be implemented as soon as possible.
- Developed **technologies should be applicable as much as possible to different vertical application** domains (identified in the SRIA), but should also be easily adapted to the specific needs of other verticals
- "**Reference Potential Customers" or "Targeted Users"** should be clearly identified in each proposal / project, in particular for demonstrators, and should be part as much as possible of requirements gathering process and validation of the solution.
- **Top down approach**: from main vertical application / users' needs, based upon transversal infrastructures (applicable to any sector), leveraging upon basic components, all in an improved ecosystem able to understand the challenges and use innovative solutions.

Linking demand and supply



From users' needs to priorities
➔ Proposed mechanisms for SRIA implementation

Analysis of main applications (input from users), **strategic for security or economic reasons** (vertical applications should drive the developments of future solution)

- market analysis and impact of cyber threats;
- concrete overall needs for the application to be shown in main demonstrators using existing technologies;

➔ **Demonstration Projects**: demonstration of available solutions in specific vertical domains to provide national security, protect economic relevant EU market sectors, allowing economies of scale through engagement with users/demand side industries and bringing together a critical mass of innovation capacities (TRL 6-9)

Transversal infrastructure supporting the applications: gaps to be filled due to evolving needs in the different applications;

➔**Transversal infrastructures (infrastructure intended as systems providing essential services for the protection of the network)**: projects able to integrate sector-neutral technological building blocks with maximum replication potential, to tackle transversal challenges (common to different applications) (TRL 6-9)

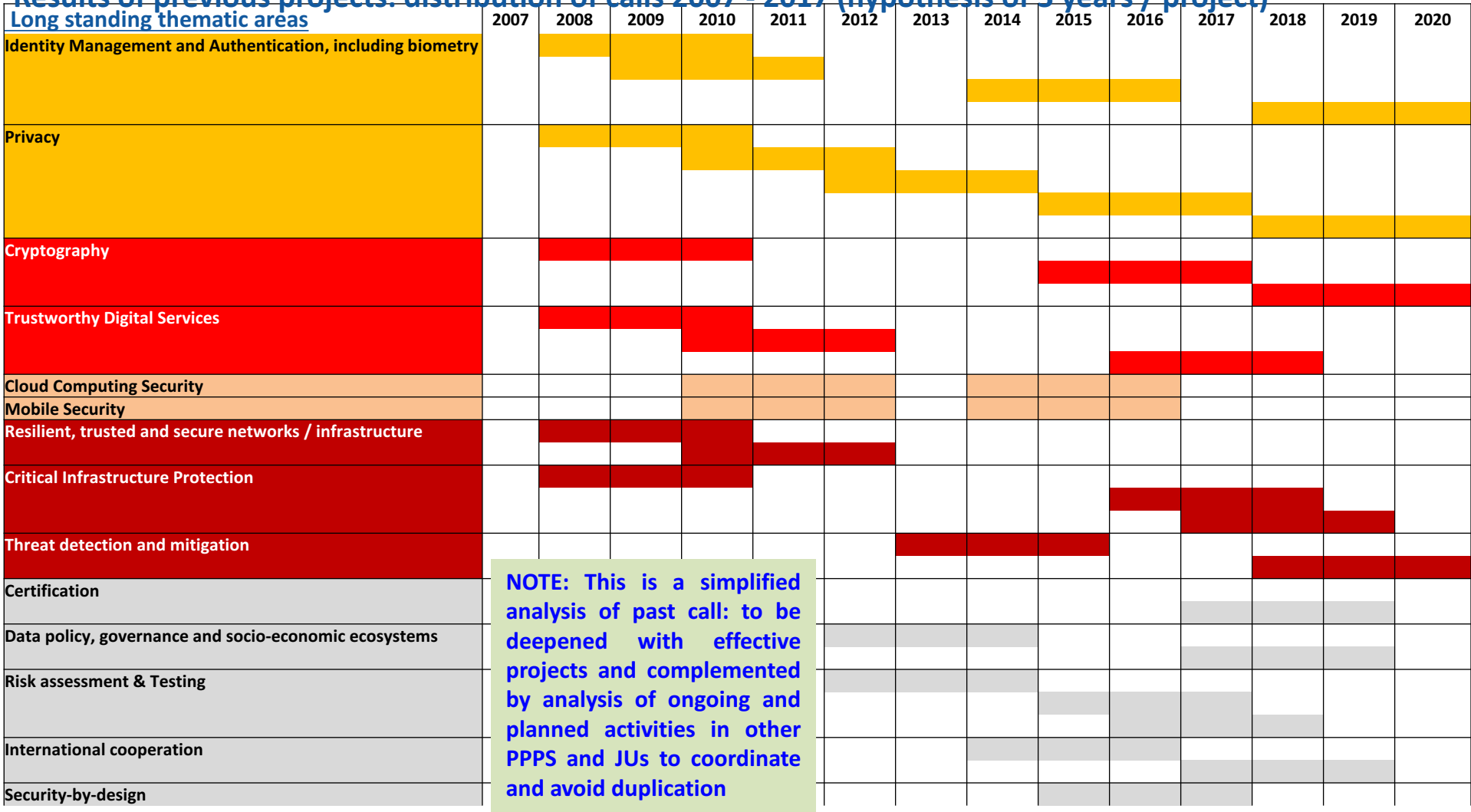
Basic technologies: gaps to be filled to support evolution of transversal infrastructure

➔ **Technological components**: mainly devoted to build those sector-neutral technological building blocks with maximum replication potential that can become market references at global level (TRL 3-5)

Ecosystem to protect the development and correct use of applications: education, certification etc.

➔ **Ecosystem:** socio-technical projects for the development of an ecosystems favourable to better implement and use innovative solutions, protect applications, increase education and awareness in the society

Results of previous projects: distribution of calls 2007 - 2017 (hypothesis of 3 years / project)



Clustering priorities

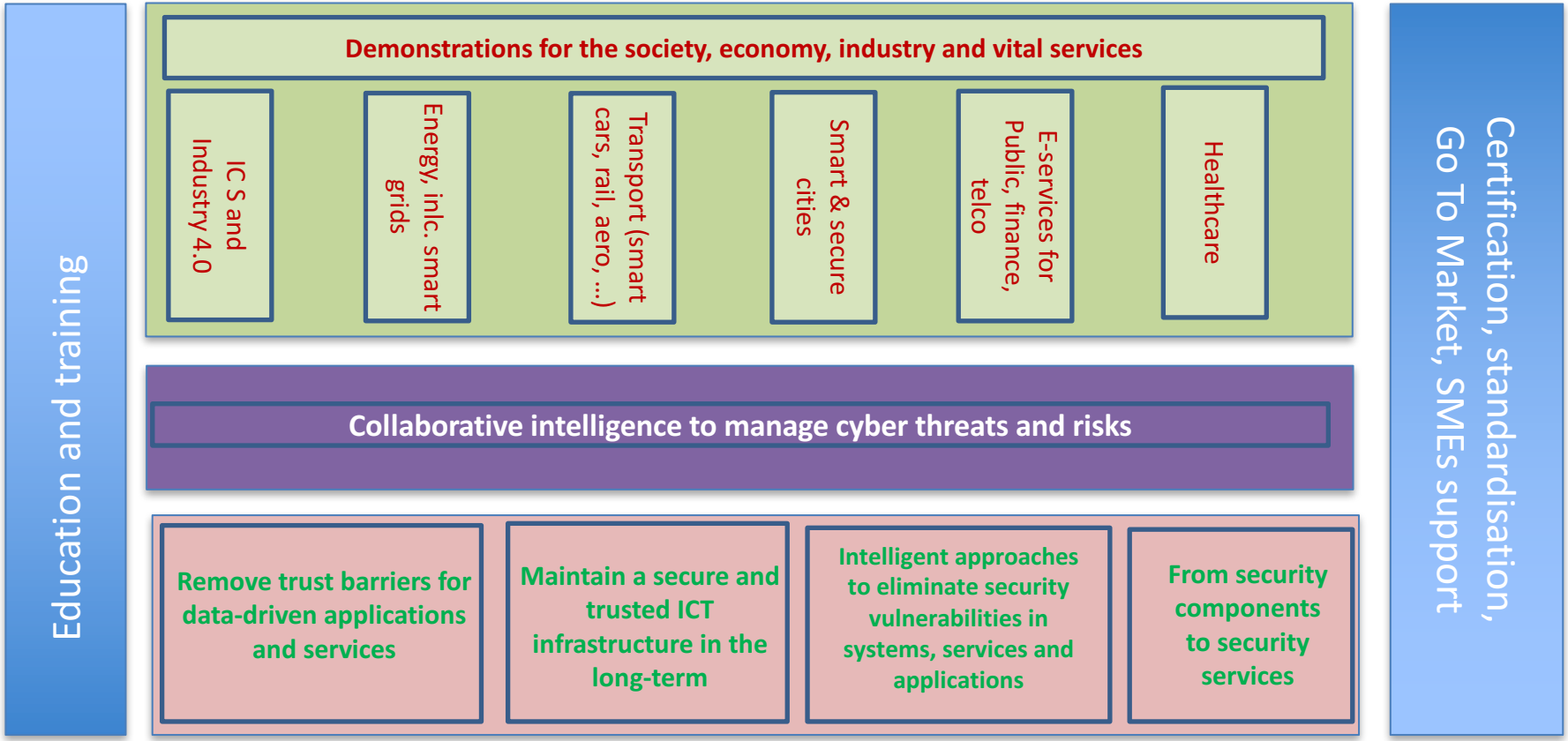
- **4 main thrusts:**
  1. Developing a **European Ecosystem** for the Cybersecurity Market and Digital Society
  2. Applying cybersecurity **technologies and infrastructures** for **protecting vital societal services and the economy**
  3. Developing European **trustworthy cyber solutions for supporting the European cybersecurity strategies** (and policies)
  4. Increase **European excellence and competitiveness** on cybersecurity

- **7 main thematic priority areas (practically the full spectrum of needs, clustered in main areas):**
  - Ecosystem for Education, training, certification, standardisation, market and SMEs growth
  - Demonstrations for the society, economy, industry and vital services
  - Collaborative intelligence to manage cyber threats and risks
  - Remove trust barriers for data-driven applications and services
  - Maintain a secure and trusted ICT infrastructure in the long-term
  - Intelligent approaches to eliminate security vulnerabilities in systems, services and applications
  - From security components to security services

Detailed structure: 7 main thematic priority areas

- 1 European Ecosystem for the Cybersecurity
  - Cyber Range and simulation
  - Education and training
  - Certification and standardisation
  - Dedicated support to SMEs
- **2 Demonstrations for the society, economy, industry and vital services**
  - Industry 4.0
  - Energy
  - Smart Buildings & Smart Cities
  - Transportation
  - Healthcare
  - E-services for public sector, finance, and telco
- **3 Collaborative intelligence to manage cyber threats and risks**
  - GRC: Security Assessment and Risk Management
  - PROTECT: High-assurance prevention and protection
  - DETECT: Information Sharing, Security Analytics, and Cyber-threat Detection
  - RESPONSE and RECOVERY: Cyber threat management: response and recovery
- **4 Remove trust barriers for data-driven applications and services**
  - Data security and privacy
  - ID and Distributed trust management (including DLT)
  - User centric security and privacy
- **5 Maintain a secure and trusted infrastructure in the long-term**
  - ICT protection
  - Quantum resistant crypto
- **6 Intelligent approaches to eliminate security vulnerabilities in systems, services and applications**
  - Trusted supply chain for resilient systems
  - Security and privacy by-design
- **7 From security components to security services**

Main thematic priority areas



Elements to prioritise the different topics

- Needs **/ challenges.** Present how threats / needs could evolve in the coming period (2018 – 2025, i.e. the time of the max extension of the coming projects)
- Status: Previous / ongoing EC projects; previous calls; other PPPs and JUs: how to interface with them
- What market:
  - Application(s) / verticals / infrastructure concerned: market size (incl. market timeline)
  - Size of the cyber threats to the verticals / infrastructure concerned
  - Potential size of the generated cyber solutions
- Why Europe: would be a leader in this area? What European added value?
- Objectives / **Scope**
  - Main "final" objective (wrt timeline): what steps are needed to reach this? E.g. certification of products (existing and future); evolving infrastructure; basic components; ecosystem (training, simulation, standards, certification, labelling …)
- **Targeted users / customers. Beneficiaries and benefits for use of the different applications / infrastructure / technologies / services**
- For the verticals: identify what are the specific needs / solutions and what are the needs / solutions in common with other verticals
- **Expected impact:** Other economic; Societal; Technological; Other
- **Budget / time / kind of project (RIA, IA; target TRL end of project)**

	2018	2019	2020	TOTAL
COORDINATION	0	2	0	2
cppp international coordination		2		2
Ecosystem (incl fast track to innovation budget)	10	17	15	42
Cyber range and simulation			10	10
Education and training	5			5
Certification and standardization	5	7		12
Dedicated support to SME		10	5	15
cyber security demonstrators in application domains	*26*	*72*	*10*	*108*
Energy, including smart grids	16			16
Transport		18		18
Healthcare		10		10
Smart & Secure Cities		13		13
Public/Finance/Insurance/Telco/ Services		16	10	26
Industry 4.0	10	15		25
Transversal infrastructures	*38*	*0*	*40*	*78*
GRC: Security Assessment and Risk Management	18			18
PROTECT: High-assurance prevention and protection	18			18
DETECT: Information Sharing, Security Analytics, and Cyber-threat Detection			20	20
RESPONSE & RECOVERY: Cyber threat management: response and recovery			20	20
Coordination of the transversal projects	2			2
Basic components	28	43	79	150
Removing trust barriers on data				
Data Security and Privacy			20	20
Identity and Distributed Trust Management	15			15
User-centric security and privacy		10		10
Maintain a secure and trusted infrastructure in the long-term				
ICT Infrastructure Protection	13		25	38
Quantum-resistant cryptography			16	16
Intelligent approaches to eliminate security vulnerabilities				
Security and Privacy by Design			18	18
Security Assurance along the supply chain		18		18
From security components to security services				
Security Services		15		15
Total	102	134	144	380

Status

- We are in line with the planned schedule and activities
  - Not an easy thask!!!!
- First SRIA delivered 1.2!
- Input to WP18-20 completed and shared with the European Commission and ECSO Public authority members for input
- It seems our input is well received from the EU and the programm commitees
  - We need to align with the new EU cyber security strategy
- We are in the phase to liaison with other cPPPs/organizations etc.

Next actions

- Routine activities:
  - Monitor implementation
  - Cooperation and coordination with other cPPP initaitivs
  - Monitoring that the WP LEIT/SC contains our topics
  - Ensuring good projects fullfilling our identified research priorities
- Align and provide actionable feedback about EU Cyber security strategy
    - Revise SRIA and suggestions to WP
- New and strategic activity
  - Next vision document for the SRIA going beyond 2020 (2027)
    - Instruments, Vision, Needs, Stakeholders,

Conclusions

- ECSO is consolidating
- cPPP SRIA WG6 and all the others WGs are actively working have clearly identified their objectives
- WG6 already delivered the main output
  - The SRIA

Additional material

- A few slides describing more into the details the tranversal infrastructures

Transversal infrastructures

Collaborative intelligence to manage cyber threats and risks

Sub-topics:

- Security Assessment and Risk Management
- High-assurance prevention and protection
- Information sharing, security analytics and cyber-threat detection
- Cyber threat management: response and recovery

CSA:

- Ensure consistency of approach and that results from sub-topics are interoperable and integrate to form a cybersecurity infrastructure reference platform
- Co-ordinate with Vertical demonstrator activities and relevant PPPs (e.g. 5GPPP)

Sub Topic: Security Assessment and Risk Management

Challenges

- High complexity and inter-dependence of digital infrastructure
- Evolving and escalating threat environment
- Measuring (lack of) security and effectiveness of controls are both difficult
- Need for dynamic risk assessment to allow timely decisions. Decision timescales shrinking

Scope

- Ref. implementation of platform for risk-based oversight and co-ordination of cybersecurity operations
- Ensure policies of the parent organisation are followed and legal obligations and commitments re fulfilled. Assess overall risk exposure and ensure that it is in line with risk appetite.
- Automated risk assessment, including impact analysis and calculation of secure network rating
- Collaborative risk assessment, dynamic sharing of threat intelligence

Expected Impact

- Support implementation of the NIS Directive
- Increased cost-effectiveness of cybersecurity investment at the corporate and national levels
- Improved cybersecurity co-operation at industry, national and European levels.

Budget/Time/Project:

- 1 project; 18 ME; IA; 2018; TRL 5-6 at start, TRL 7 or higher at the end of the project

Sub Topic: High-assurance Prevention and Protection

Challenges

- Lack of trust and confidence in digital infrastructure is hindering ongoing digital revolution
- Size, heterogeneity, dynamism and complexity of digital infrastructure increasing
- Many new devices, applications and services not designed with security in mind
- Vulnerabilities expose end-users to attack, eroding trust in digital services and infrastructure

Scope

- Reference implementation of trustworthy digital infrastructure platform
- Protect digital infrastructures and the applications that use them by preventing cyber-attacks being successful
- Integrated, holistic approach including minimisation of attack surfaces, trusted and verifiable computation systems, secure runtime environments, assurance, verification tools and secure-by-design methods.
- Take into account technological and business innovation trends that are converging to revolutionise the nature of digital infrastructure.

Targeted users

- Technology and service providers, system integrators, critical infrastructure providers, certification authorities

Expected Impact

- Increase the trustworthiness of European ICT services and products and competitiveness of industry

Budget/Time/Project:

- 1 project; 20 ME; IA; 2018; TRL 5-6 at start, TRL 7 or higher at the end of the project

Sub Topic: Information Sharing, Security Analytics and Cyber-threat Detection

Challenges

- Not all attacks can be prevented so must assume systems penetrated and actively search for evidence
- In 2015, the median time from penetration of a network by attackers to their discovery was **146 days** (Mandiant)
- Advanced attackers evolve techniques continually, so need to be able to detect novel attacks
- Must share threat intelligence to learn collectively, but concerns over blame and leakage of sensitive information
- How to extract actionable information from large amounts of heterogeneous low-level security data?

Scope

- Ref. implementation of platform to anticipate, detect, diagnose and investigate actual and potential attacks.
- Collection and analyse of data from appliances, logs, open source intelligence, etc. to extract knowledge
- European network for *collaborative* threat intelligence and responses
- Advanced means of detecting system anomalies and integrity violations. Intelligent, 'Big data' security analytics

Targeted Users

- Cybersecurity product and service vendors, system integrators, infrastructure operators, CERTs

Expected Impact

- Better identification of advanced attacks and responding more quickly and effectively to them
- NIS Directive is enabled
- Innovation opportunities for European cybersecurity product and service vendors

Budget/Time/Project:

- 1 project; 20 ME; IA; 2020; TRL 5-6 at start, TRL 7 or higher at the end of the project

Sub-topic: Cyber threat management: response and recovery

Challenges

- The information on which to base decisions is often incomplete, uncertain or conflicting.
- The speed at which attacks take place is accelerating – automation is needed but cannot be trusted
- Response and recovery actions require great care as mistakes can lead to higher damages than original attacks
- Tools are often poorly integrated – human analysts are the integration layer
- Attackers may modify their tactics depending on the response of defenders.

Scope

- Reference implementation of a Response and Recovery platform able to combat future threats
- Risk- and cost-based approaches to response and recovery, supported by Threat Intelligence
- Automated execution of SOC analysts' high level decisions in terms of low level actions to combat attackers
- Leverage virtualisation (SDN, etc.) to enable adaptive response (e.g. 'moving target defence') and recovery
- Real-time predictive tracking of attacks, attack attribution, forensics

Targeted Users

- Cybersecurity vendors, managed-service providers, ICT infrastructure providers, end-user organisations

Expected Impact

- Interoperable or integrated response and recovery products and services available on the market, enabling robust, resilient, reliable and trustworthy ICT services for end-user organisations
- Respond to threats in a timely fashion, minimise the impact, and restore normal operation smoothly
- Effective approaches and tools for Response and Recovery operations in cloud and hybrid infrastructures

Budget/Time/Project:

- 1 project; 20 ME; IA; 2020; TRL 5-6 at start, TRL 7 or higher at the end of the project