ANNEX: DETAILED ECSO ACHIEVEMENTS, ONGOING ACTIVITIES AND IMPACT

**General Achievements: ECSO is already present!**

- **Membership:** From initial 132 members mid-2016 to about 250 contributing members end 2018 representatives of all main public and private sectors ➔ **IMPACT:** ECSO is already a structured European Community, reaching via its members (including Association) more than 2000 organisations.

- **Strategy:** Starting from sometimes diverging opinions and interests from different stakeholders we manage to define a common strategy, objectives, priorities and actions for the development of an EU cyber security ecosystem ➔ **IMPACT:** ECSO has a common and comprehensive strategy for future investments and policy implementation.

- **Governance:** Set up of a governance and internal rules, providing a fully transparent, balanced and democratic decision-making process among different category of stakeholders ➔ **IMPACT:** ECSO is running European Public-Private tool in the hands of its members and of EU Institutions.

- **Working Groups:** Development of a real Public-Private dialogue and cooperation through ECSO Working Groups policy resulting in concrete activities ➔ **IMPACT:** ECSO is running Working Groups tackling current political, legislative and technological topics for a true European cyber security industrial policy.

- **EU Cooperation:** Dialogue / Cooperation with EU and International Institutions: E.Parliament; Council / Horizontal Working Party on Cyber (regularly invited to present positions and updates); European Commission: VP / Commissioners and Cabinets (Gabriel; Ansip; King, Oettinger), CNECT, MOVE, ENER, HOME, JRC, REGIO, GROW; Agencies: ENISA, EUROPOL, EIT, EIB, EASA, eu-LISA, FRONTEX; EDA; EEAS; Programme Committees; International Organisations (ITU, WEF, ...); dialogue with Council’s HWP on cyber and past / present / future EU Presidencies (ECSO in the “Trio objectives”) ➔ **IMPACT:** ECSO is already a European Hub to collect, digest and transfer common views and priorities to EU and national Institutions and stakeholders. **ECSO is already supporting Networking and Coordination of national and regional bodies (administrations / private stakeholders).**
  - **Recommendations to E. Institutions on:** cyber security package (Cybersecurity Act: role of ENISA and EU Cybersecurity Certification Framework), priorities for future MFF investments on cyber security; R&I priorities for H2020 (cPPP); Industrial Cyber Security Policy; and the Network of Competence Centres ➔ **IMPACT:** Effective use of ECSO recommendations and priorities in EU policies and programmes.

- **Communication:** Wide communication and dissemination activities, internal (among members) and external (on average, we deliver our messages about in one conference per week) ➔ **IMPACT:** ECSO is delivering messages and positions every day around Europe.
ECSO Working Groups achievements: Policy suggestions and concrete activities

**WG1 – Standardisation, Certification, Labelling and Supply Chain Management**

- **Support to the EU Cybersecurity Certification Framework and Trusted Supply Chain in Europe**
  - Tool: SOTA, COTI reports - SOTA: State of the Art in Europe on certification for the different products and services; COTI: needs from industry for future certification ➔ **IMPACT**: Better common understanding of situation and needs to prepare future priorities
  - Tool: Meta-scheme: input to the Cybersecurity Act. Tool for qualitative market analysis to define focused initiatives and promote EU solutions as methodology for the European Certification Framework ➔ **IMPACT**: Used by the Council’s HWP to find the Compromise Agreement.
  - Tool: Priorities for future EU certification schemes (under development). Suggestions to ENISA ➔ **IMPACT**: Provide ENISA with common priorities for definition of certification schemes on products, process and services

- **Support to EU standardisation on cyber security**
  - Tool: MoU with CEN/CENELEC. Definition of priorities for developing EU standards ➔ **IMPACT**: Simplify tasks for CEN/CENELEC to initiate standardisation, in particular linked to certification.

**WG2 – Market Deployment, Investments and International Collaboration**

- **Cyber Security Market Knowledge** ➔ **IMPACT**: Better understanding of the EU cyber security stakeholders, products and services. Easier identification of EU solutions and providers for investments.
  - Tool: ECSO Cyber Security Market Radar ➔ **IMPACT**: Qualitative market knowledge and analysis (open to any EU stakeholder).

- **Investing in cyber security (and in particular in SMEs)** ➔ **IMPACT**: Boost EU investment (in particular for SMEs) in the cyber security market; develop private funding model for cyber security (including capital ventures and insurances).
  - Tool: ECSO Cyber security matchmaking events between investors and SMEs / start-ups / scaleups (jointly with WG4) ➔ **IMPACT**: Effective link between investors (large companies, banks, capital ventures and SMEs) in view of future investments.

- **International cooperation**. Dialogue with Japan and other Third Countries on a case by case basis ➔ **IMPACT**: Identification of synergies and cooperation with Third Countries; promotion of EU technology and competence at international level.

- **cPPP Monitoring 2016-2017. cPPP commitments wrt the EC; leverage factor >3** ➔ **IMPACT**: Stimulate investments and cooperation among stakeholders on SRIA topics.
**WG3 – Sectoral Demand**

- **Identification of vertical / users’ needs**: ECSO sectoral reports for identification of sectoral and cross-sectoral needs for Industry 4.0 and ICS, Finance, Healthcare, Smart Cities, Energy (eGov, Telecom/Media and Transport under finalisation) and impact analysis of the legislation & regulations for different verticals (new specific transversal Task Force to be set up on legislative issues) ➔ **IMPACT**: Priorities and sector-specific requirements that can be used for definition of R&I and capacity building / process development and investments.
  - **Tool**: Sectoral reports developed by WG3, in cooperation with the other WGs
  - **Tool**: ECSO sector-specific workshops. Deep dive on needs, requirements and threats of a specific sector, with participation of relevant external (non ECSO members) sector associations, users, and EU DG’s and agencies (also to build up the Community).

- **Sensitive needs knowledge, threat sharing and crisis management ➔ IMPACT**: Improved incident reporting, information sharing and crisis management for verticals, satisfying NIS-D and other EU regulations needs, across different EU countries; deeper identification of sensitive needs and occurred cyber threats
  - **Tool**: ECSO Users Committee. Trusted forum restricted to users to exchange sensitive information on cyber threats and identify needs
  - **Tool**: Position paper with analysis of ISACs’ needs. Assessing needs and priorities for a European ISAC. Analysis made across the different sectors, also considering interdependencies.
  - **Tool**: Common Application Platform for users (under development). Harmonised incident reporting and threat sharing across Europe.

**WG4 – Support to SMEs, coordination with countries (Eastern and Central EU in particular) and regions**

- **Support to SMEs**
  - **Tool**: SME Hub (under development) ➔ **IMPACT**: Provide SMEs with higher visibility on the market (partnership, joint offering, marketing, labelling) and investment opportunities
  - **Tool**: Access to Market and Finance matchmaking events (in cooperation with WG2) ➔ **IMPACT**: Investment opportunities for European SMEs also to retain them in Europe.

- **Support to EU Regions**
  - **Tool**: EU Projects for inter-regional acceleration programme (S3I Pilot Action Project, INTERREG Europe CYBER 2018-2023) ➔ **IMPACT**: Harmonisation of priorities across EU regions for regional approaches (toward smart specialisation) for access to market with increased local participation of SMEs and end-users (including education bodies) with future support from EU regional funds.

- **Cooperation with East Europe (under development)**. Mapping initiatives in Central and Eastern Europe (CEE) ➔ **IMPACT**: Develop cooperation with East EU SMEs and clusters to promote the development of local skills and cyber security ecosystem. Action plan for regional markets.
WG5 – Education, Training, Awareness, Cyber Ranges

- EHR4CYBER (European Human Resources 4 Cyber): developing European Skills, Jobs and Awareness on Cyber Security.
  - Tool: Papers on Gaps in Education & Professional Training and Certification ➔ IMPACT: Awareness and suggestions for coordination at EU level in education and training
  - Tool: ECSO’s Women4Cyber initiative ➔ IMPACT: Enhance participation, role and positions of women in cyber security
  - Tool: Pilot for the job platform EHR4CYBER job platform (under development in regions’ project) ➔ IMPACT: Support job creation and link to local job platforms.
  - Tool: European Cyber League (under discussion): Development of cooperation among European cyber specialists (individuals) ➔ IMPACT: Leverage the development of Europe in cyber security also through individual competences.
  - Tool: Awareness workshops ➔ IMPACT: Enhance the level of awareness and cyber hygiene for targeted audiences (citizens, policy-makers, CISOs, etc.)

- Cyber Ranges workshop series. Approach and methodology on cyber ranges in cooperation with the European Defence Agency and ECSO members ➔ IMPACT: Federation of cyber ranges.

WG6 – Strategic Research and Innovation Agenda (SRIA), innovative technologies and synergy with cyber defence

- Strategic Research and Innovation Agenda for 2017-2020 R&I priorities. Compliance with cPPP commitments ➔ IMPACT: The ECSO SRIA has been largely adopted in 2017-2020 H2020 ICT work programme

- Scenarios and priorities for Horizon Europe (ECSO 2020-2027 vision – under development) ➔ IMPACT: ECSO input (also to the future ECC) for definition of future priorities for R&I in Horizon Europe and DEP investments
  - Tool: Scenario definitions: Society and Citizen (social good); Data and Economy; Disruptive Technologies; Digital Transformation in Verticals.
  - Tool: Technical papers: on Artificial Intelligence, Internet of Things, Blockchain. Advice on main disruptive technologies and basis for cooperation with other cPPP (BDVA, AIOTI, euRobotics, EFFRA, 5G) and new EU initiatives (DEP)

- Facilitating collaborative research projects. Brokerage events to prepare common proposals for H2020 ➔ IMPACT: Provide members (and non-members – i.e. the interested Community) the possibility to liaise and set up H2020 proposals closely linked with the cPPP and ECSO objectives (e.g. Pilots for Competence Centres)

- Synergies Cyber Security wrt Cyber Defence (under definition). Understanding interests to link with future EC activities and organisations ➔ IMPACT: Maximise impact of R&I investments in cyber security technologies.