
# European Cyber Security Organisation (ECSO)

**Fabio Martinelli (CNR)**

ECSO WG6 co-chair

Concertation Meeting

26 April *2018 – Brussels*

# Europe and cybersecurity: now evolving faster. Overview of the context

- 2013: EU Cybersecurity Strategy
- 2013: NIS Platform
- 2014: Digital Single Market / Digitalisation
- 2016: cPPP on Cybersecurity
- 2017: Joint Communication on EU strategy Review and Cybersecurity Act ("New" EU Cyber Security Agency: ENISA + EU Certification Framework)
- New technologies: Artificial Intelligence / Big Data Analytics; IoT; High Performance Computing…
- Still large number of Bodies and fragmentation at EU and MS level
- Creation of a Network of Cybersecurity Competence Centres (pilots starting in 2018) with a European Cybersecurity Research and Competence Centre (ongoing EC call for proposals)
- EC proposal for the next MFF (2021 – 2027): May 2018 (details for cyber expected mid June)
- Transposition of the NIS Directive and application of the GDPR Regulation: May 2018
- Possible evolution of the cPPP (after 2020) towards a more ambitious governance and objectives

# ABOUT THE EUROPEAN CYBERSECURITY PPP

## A EUROPEAN PPP ON CYBERSECURITY

The European Commission has signed on July 2016 a PPP with the private sector for the development of a common approach and market on cybersecurity.

## 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.

## BUDGET

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). Cybersecurity market players are expected to invest three times more (€ 1350 mln: leverage factor = 3) to a total up to €1800 mln.

## SUPPORT

European Cyber Security Organisation – ECSO Association has been created to engage with the EC in this PPP.
ECSO is open to any stakeholder (public / private; user / supplier) allowed to participated in H2020 projects.

# ABOUT ECSO

**The ECSO approach is going beyond the work of a typical Association supporting a cPPP, as it tackles, on top of Research & Innovation issues, all those topics that are linked to the market development and the protection of the development of the Digital Single Market, in the frame of the European Cybersecurity Strategy.**

The uniqueness of ECSO is to include among its members (also at Board of Directors level and within the working groups*) **high representatives and experts from national and regional public administrations**. This approach is fundamental

- in a sector dealing with "security" as application of cybersecurity is and will remain a sovereign issue.
- **to increase the quality of the ECSO recommendations** to the European and national institutions → allowing a faster decision making by public bodies and a viable implementation by the private sector of the decisions taken (regulations, standards etc.).

For this reason **ECSO itself is a public – private body**, creating a **new and dynamic multi-stakeholder dialogue**, preparing for the future evolutions and needs in this sector, as envisaged in the EU cybersecurity strategy.

***ECSO working groups are dealing with the different aspects of what we call "cybersecurity industrial policy"**

# ECSO membership overview

132 founding members: now we are **236 organisations from 29 countries and counting (included 6 new provisional membership – in brackets)**

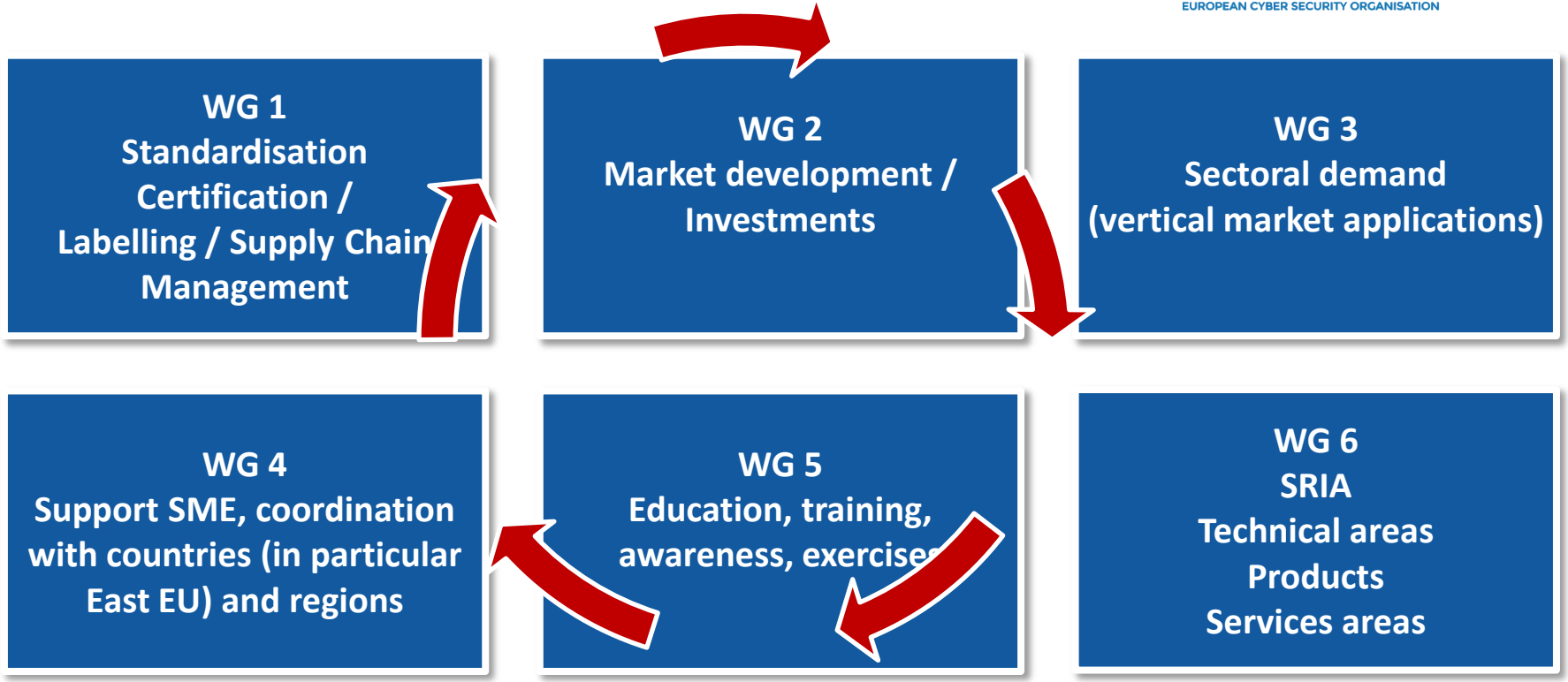
| | | | |
|---|---|---|---|
| AUSTRIA | 7 | ITALY | 26 (+2) |
| BELGIUM | 13 | LATVIA | 1 |
| BE - EU ASSOCIATIONS | 9 | LITHUANIA | 1 |
| BULGARIA | 1 (+1) | LUXEMBOURG | 4 |
| CYPRUS | 4 (+1) | NORWAY | 4 |
| CZECH REP. | 3 | POLAND | 6 |
| DENMARK | 5 | PORTUGAL | 3 |
| ESTONIA | 7 | ROMANIA | 1 |
| FINLAND | 8 | SLOVAKIA | 2 |
| | | SLOVENIA | 1 |
| FRANCE | 24 (+1) | SPAIN | 32 |
| GERMANY | 21 | SWEDEN | 2 |
| GREECE | 5 | SWITZERLAND | 5 |
| HUNGARY | 3 | THE NETHERLANDS | 17 |
| IRELAND | 3 | TURKEY | 3 (+1) |
| ISRAEL | 2 | UNITED KINGDOM | 8 |

- Associations : 21
- Large companies and users: 70
- Public Administrations: 20

  AT, BE, CY, CZ, DE, EE, ES, FI, FR, IT, SK, FI, NL, NO, PL, UK, BG, SE, GR +

  observers at NAPAC (DK, HU, IE, LT, LU, LV, PT, RO, SI, MT, …)
- Regional clusters: 6
- RTO/Universities: 62 (+1)
- SMEs: 52 (+5)

# Working Groups



# Main achievements / deliverables in the first 21 months of the cPPP and ECSO

- **WG1** (135 members with 289 experts): Initial positions for an EU certification framework: SOTA, COTI, Meta-Scheme. Initial cooperation (MoU) with CEN/CENELEC – ETSI for standards
- **WG2** (81 members with 153 experts): Market analysis: Support Cybersecurity Industry Market Analysis (CIMA project led by EC-PWC-LSEC). Investments: initial discussions with banks & insurances; support to national bodies to understand and develop investments for start-ups. International cooperation: dialogue with US; involvement via members in EC CSA projects (Japan and US)
- **WG3** (121 members with 266 experts): SOTA under finalisation; involvement of DG ENER in the cPPP; initial dialogue with ISACs (finance, energy); more concrete activities under definition.
- **WG4** (80 members with 141 experts): SME – Position paper (role of SMEs in the cybersecurity ecosystem); Regions – partner as advisor in proposal for INTERREG (with 7 regions: ECSO members and not). Support to proposal for thematic partnership in Interregional cooperation in cybersec domain (5 regions)
- **WG5** (98 members with 202 experts): Initiation of a EHR-4CYBER Network; mapping of educational and professional training courses; started tackling gender issues on education & training
- **WG6** (157 members with 351 experts): Defining research priorities: SRIA. One year after: analysis review of technology and needs evolution. Link with other PPPs (BDVA, EFFRA, 5G).

# 21 months after: Update of the analysis of the situation

**Evolutions in the latest months**

- Evolution of the awareness on cybersecurity at national and EU level
- Evolution of threats (e.g. Mirai/ IoT; WannaCry, Spectre & Meltdown) and priorities (political: interferences in democratic processes)
- Evolution in the dialogue between public and private stakeholders thanks to the cPPP / ECSO (but still limited exchange of information due to sovereignty or competition issues)
- Revised objectives / actions of the EU cybersecurity strategy
- Definition / implementation of new legislations (NIS Directive, GDPR, ePrivacy, …)

**Digitalisation of the industry, of infrastructures and of the society: need for increased cybersecurity**

- Impact on all levels: societal and economic
- Strongly increased need for skilled experts (c.f. EC Joint Comm: 350.000 by 2022)
- Need for improved control / ownership / security of data in Europe
- Growth of pervasive and distributed IT infrastructure (secure IoT, 5G, Cloud) needing local and fast reaction capability
- IT Infrastructure for centralised information (e.g. SOC as platform for security services managed by MSSP and CERTs) to increase wider (/global) security and detection / remediation aspects: Big Data Analytics / Artificial Intelligence
- Virtualisation of networks and software defined services (including security); increased use of blockchain (DLT)

# INDUSTRY OBJECTIVES for the cPPP strategy

**Industry looks for:**

- Investments in the development of innovative cybersecurity technologies;
- Validation of the solutions in key infrastructures and applications;
- Rapid reaction capabilities in case of attacks
- The development of a sustainable ecosystem that will facilitate innovation uptake including:
  - Increased investments and awareness for capacity building at regional, national and EU level
  - European certification framework
  - Education and harmonised training for increased needs in job creation
  - Increased leverage upon SMEs
  - Development of cybersecurity services

# Main ECSO activities envisaged for 2018

- **WG1:** Support to the establishment of the European Cyber Security Certification Framework; update SOTA, COTI and Meta-Scheme; cooperation (MoU) with CEN/CENELEC & ETSI and ENISA; Work on common schemes for different sectors in coop. with WG3
- **WG2:** Radar of European solutions (national catalogues for DE, SP, FR, ES, UK); Directory and Marketplace using common taxonomy in coop with WG6; recommendations for EU investment model – link with WG4 (envisaging an ECSO investment fund for start-ups); Mapping of events and main stakeholders in CS; Monitoring and report on cPPP implementation / investments
- **WG3:** Sector specific reports on users' needs / SOTA; Report on NIS implementation and harmonisation of incident reporting; Sector-specific guidelines on implications of GDPR on cybersecurity and privacy; Support to ISAC's implementation; envisaging operational platforms
- **WG4:** Link VCs and Investors to Start-Ups and SMEs (local events in Paris, Berlin and Brussels). Marketplace and tool for community building and tools for funding opportunities and projects; SME label "made in EU"; Register of EU cybersecurity SMEs; SME Hub platform and "European (ECSO) Cyber Quadrants"; cooperation and link with / specialized regions for concrete activities (e.g. supporting local SMEs and start-ups' access to market; education / training); Support increased coordination and participation of East EU bodies
- **WG5:** Participation in Digital Opportunity pilot scheme; Support to the « School of the Future » initiative and enlarge message to Europe for students' education before University level. Development of EHR-4CYBER network with share of needs, professional certification mapping, best practices and pushing creation of national (EU?) CS academia
- **WG6:** **Work on global trends and key implications on strategy through 2027; SRIA 2.0; Studies on R&I needs on specific verticals; Link with relevant cPPPs to coordinate strategy for EU cybersecurity R&I; Support to creation of NCCC; New Scientific & Tech. Committee**
- **NAPAC:** Contribution to standards & certification (WG1) for EU framework; support growing education and training at national level (WG5); Dialogue with WG6 for review of R&I priorities; supporting the set up of the Network of Cybersecurity Competence Centers (NCCC)
- **PARTNERSHIP BOARD:** Suggestions for the NCCC and the ECRCC (European Cybersecurity Research Competence Centre); initial dialogue on review of 2020 priorities and set up of FP9; monitoring of the cPPP

# WG6: SRIA -
# Technical areas, Products, Services areas

## 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

- **Coordination of results and expectations from EC R&I projects**
- **Coordination of cybersecurity activities across cPPPs and EIT**
- **Support cPPP implementation and H2020 cybersecurity projects**
- **Detailed suggestions for the WorkProgramme 2018 - 2020 using an updated and focussed SRIA**


## Synthesis of activities

SRIA delivered to the European Commission as input for the 2018 – 2020 H2020 Work Programme: good acceptance of suggested priorities.
The Programme Committee decided to put more money on basic / transversal technologies than on specific pilots / applications. Work on taxonomy with WG2 and soon with JRC

**ECSO STRATEGIC RESEARCH & INNOVATION AGENDA v1.2**

→ cPPP SRIA v1.0 and industry proposal as initial guidelines
→ Available on ECSO website: https://www.ecs-org.eu/documents/publications/59e615c9dd8f1.pdf

# 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**

ECS
EUROPEAN CYBER SECURITY ORGANISATION

ECSO SRIA input to

- LEIT ICT WP 2018-2020 (Cybersecurity and more)
- Secure Societies – Protecting freedom and security of Europe and its citizens

# WG6: SRIA priorities for R&I

## STRATEGIC PRIORITIES

- **Cybersecurity Technologies & Services**
- **Infrastructure & Applications**
- **Cyber ecosystem**

EUROPEAN CYBER SECURITY ORGANISATION

## CYBERSEC TECHNOLOGIES & SERVICES to protect Infrastructure / Applications and citizens' privacy

- Encryption (key management, homomorphic, post quantum, …)
- ID and DLT (blockchain, …) security
- AAA: Authentication; Authorisation; Accounting
- Security / Resilience & Privacy by Design (GDPR, …)
- PET: Privacy Enhancing Technologies
- Information Sharing, Threat Detection and Intelligence (incl. sensors / probes for ICS, SIEMs and SOCs), Artificial Intelligence and Analytics
- Protection of innovative ICT infrastructure
- Risk Management, Response and Recovery
- Tamperproof communication protocols

## Pilots and validation of solutions in INFRASTRUCTURE (for use in all sectors) & APPLICATIONS (specific verticals)

- Industry 4.0 (FoF, Robotics, SPIRE, AIOTI, ECSEL)
- Energy (EdB; AIOTI)
- Transport (AIOTI, ECSEL)
- Finance (EU FI-ISAC)
- Public Administration (EU Cloud Initiative; FIWARE, HPC, BDV)
- Health (EIP AHA, AIOTI, ECSEL)
- Smart cities (Smart Cities and Communities; EIT Digital, EdB, AIOTI, ECSEL)
- Telecom (5G; AIOTI)

## CYBER ECOSYSTEM: preparing the market to introduce and use innovations

- Standardisation
- Validation / Labelling / Certification (end user awareness for implementation; different needs and different levels, flexibility for evolution)
- Trusted management of the supply chain: Assurance
- Education (cyber-Erasmus)
- Training/ simulation (certification of experts to help employment needs)
- Awareness of citizens, users (Cyber Hygiene) and decision makers (procurement, implementation and use);
- Legislation & Liability
- Investments – Funds / Economics - Business models / Insurances
- Support to SMEs
- Regional / local aspects

# WG6 - Detailed overview of WG6 activities

**Synthesis of latest activities**

- Work with other PPPs and similar EU activities to coordinate cyber security objectives (BDVA, EFFRA, 5G IA, EURobotics, IoT Forum / AIOTI, ..)
- Ongoing activity: focus on cyber security strategy priorities for update of SRIA and identification of priorities beyond 2020
    - Work on the methodology and scenario building approach – global trends and key implications through 2027
        - Areas of interest are: Society and Citizen (Social Good); Data and economy; Artificial intelligence & Disruptive Technology; Digital Transformation in Verticals
    - Identified the importance to align the strategy with the industry vision to sustain the digital transformation of the society and economy
    - Established dialogue with ENISA and EDA on research priority for the future (presentations at the last WG6 meeting / January 2018 and ongoing discussions)
- Discussion about the Network of Cybersecurity Competence Centers (NCCC) (call SU-ICT-03) and potential impact. Support to members and brokerage.
    - Also checking the missing topics whose budget was used for the NCCC call
- Work on taxonomy with WG2 / WG4 and JRC (comments to JRC taxonomy sent as individual contributions of members)
- Set up of the Scientific Committee (ECSO members, cPPPs representatives, agencies representatives)

**WG6 organisation**

- Identified the need to restructure the WG6 around the 4 key drivers → to be reflected in the SWGs (rapporteurs for the scenarios identified)

# WG6 - Updated 2018 objectives and concrete deliverables

## Planned activities and objectives

- Describe scenarios focusing on global trends and key implications through 2027. Starting point will be the SWOT analysis of the SRIA topics to identify challenges and opportunities towards 2027 – New and strategic activity
- Foresight exercise for what do we want to achieve by the end of FP9
- Discussion on the future of Network of Cybersecurity Competence Centers (NCCC) with a EU Cybersecurity Research and Competence Centre (ECRCC)
- Monitoring activity: set up of the task force (members identified) and liaison with CSAs (discussion at the last WG6 meeting // January 2018)
- Identify best support mechanisms for ECSO members in H2020 project proposals

**Collaborations**

- EDA and ENISA: Reinforce dialogue on research priorities for the future (regular activities with ENISA planned)
- JRC: Revise and work on a common taxonomy (JRC / WG2 / WG4)
- 5G IA: Foreseen a join task force and technical roundtable. MoU approved by ECSO Board
- BDVA: common position paper
- EFFRA: work in light of the industry 4.0 call on security (2019) and update of the strategic agendas → technical discussions on requirements and cybersecurity solutions
- EURobotics: focus on cybersecurity challenges for robotics and interest in healthcare sector
- IoT Forum / AIOITI: joint track at IoT week to focus on cyber security challenges, data protection, and impact for vertical sectors

## WG6 planned deliverables

- Scenarios description → Internal version (June 2018) and public (December 2018)
- Joint position papers with other cPPPs → to be planned

## F2F meetings

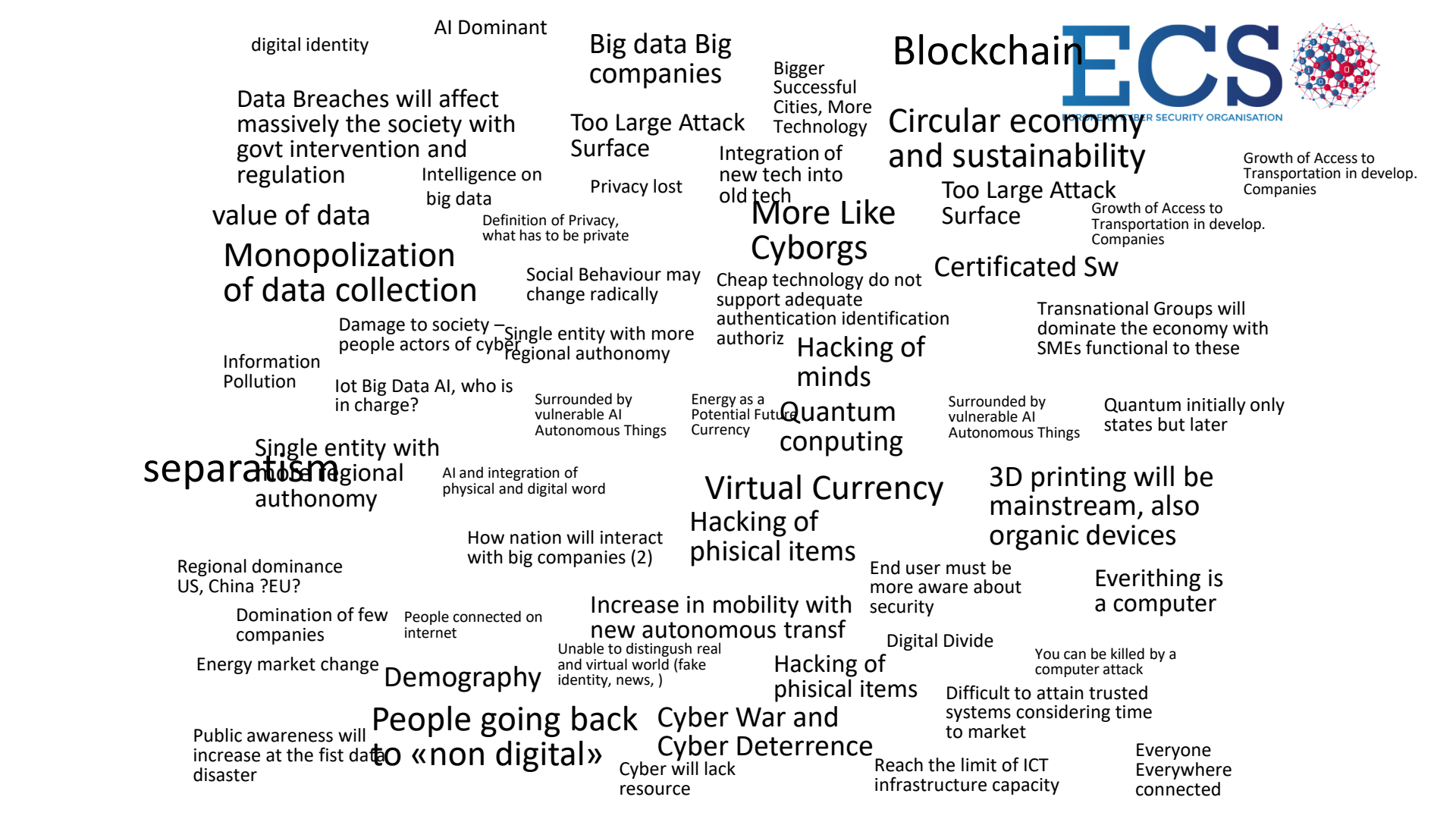
- F2F meetings back to back with the General Assembly
- Offline activity on the scenarios
- Roundtables with other cPPPs and EU initiatives

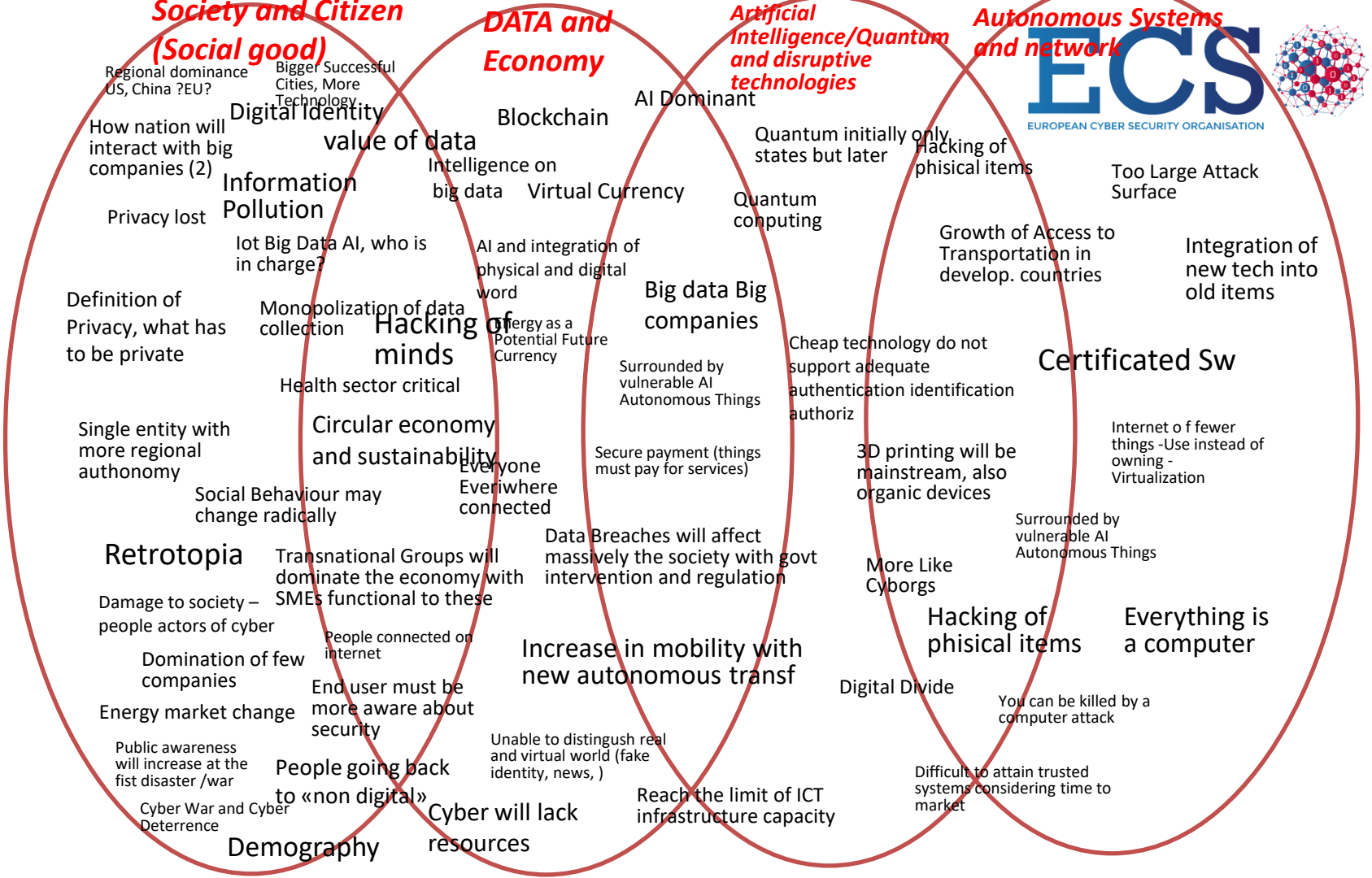
# Define the European interest and role

- What will be the global trends and key implications citizen life through 2027? What will be the main driver(considering political, economic, social, and technological PEST aspects)
  - Applying risk management-based evaluation for improbable issues relevant for each one of the global trends in terms of key implications identify what can be:
    - Possible - “might” happen (future knowledge)
    - Plausible – “could” happen (current knowledge)
    - Probable - “likely to” happen (current trends)
    - Preferable - “want to” happen (value judgements)
- Which are the cyber security threats / challenges and opportunities?
  - Refer to the initial SWOT analysis from the topics identified in the SRIA
- Who will be the end-users and what are their needs?
- Who are the potential stakeholders and what are their respective needs?
  - What will be the role of cyber security? And the role of different stakeholders (ENISA, industry, … )? This is important to address aspects related to liability.

## Initial steps

- Initial brainstorm (F2F meetings)
  - 4 scenarios identified to be revised and fully elaborated


digital identity
AI Dominant
Big data Big companies
Blockchain
Bigger Successful Cities, More Technology
Data Breaches will affect massively the society with govt intervention and regulation
Too Large Attack Surface
Circular economy and sustainability
Integration of new tech into old tech
Growth of Access to Transportation in develop. Companies
Intelligence on big data
Privacy lost
Too Large Attack Surface
value of data
Definition of Privacy, what has to be private
More Like Cyborgs
Growth of Access to Transportation in develop. Companies
Monopolization of data collection
Social Behaviour may change radically
Cheap technology do not support adequate authentication identification authoriz
Certificated Sw
Damage to society – people actors of cyber
Single entity with more regional authonomy
Transnational Groups will dominate the economy with SMEs functional to these
Information Pollution
Hacking of minds
Iot Big Data AI, who is in charge?
Surrounded by vulnerable AI Autonomous Things
Energy as a Potential Future Currency
Quantum conputing
Surrounded by vulnerable AI Autonomous Things
Quantum initially only states but later
Single entity with more regional authonomy
separatism
AI and integration of physical and digital word
Virtual Currency
3D printing will be mainstream, also organic devices
Hacking of phisical items
How nation will interact with big companies (2)
Regional dominance US, China ?EU?
End user must be more aware about security
Everithing is a computer
Domination of few companies
People connected on internet
Increase in mobility with new autonomous transf
Digital Divide
Unable to distingush real and virtual world (fake identity, news, )
You can be killed by a computer attack
Energy market change
Demography
Hacking of phisical items
Difficult to attain trusted systems considering time to market
People going back to «non digital»
Cyber War and Cyber Deterrence
Public awareness will increase at the fist data disaster
Cyber will lack resource
Reach the limit of ICT infrastructure capacity
Everyone Everywhere connected


Society and Citizen (Social good)
DATA and Economy
Artificial Intelligence/Quantum and disruptive technologies
Autonomous Systems and network
ECS
EUROPEAN CYBER SECURITY ORGANISATION
Regional dominance US, China ?EU?
Bigger Successful Cities, More Technology
Digital Identity
How nation will interact with big companies (2)
value of data
Information Pollution
Privacy lost
Iot Big Data AI, who is in charge?
Definition of Privacy, what has to be private
Monopolization of data collection
Hacking of minds
Health sector critical
Single entity with more regional authonomy
Circular economy and sustainability
Social Behaviour may change radically
Retrotopia
Damage to society – people actors of cyber
Transnational Groups will dominate the economy with SMEs functional to these
Domination of few companies
People connected on internet
Energy market change
End user must be more aware about security
Public awareness will increase at the fist disaster /war
People going back to «non digital»
Cyber War and Cyber Deterrence
Demography
Cyber will lack resources
Blockchain
Intelligence on big data
Virtual Currency
AI and integration of physical and digital word
Energy as a Potential Future Currency
Everyone Everiwhere connected
Secure payment (things must pay for services)
Data Breaches will affect massively the society with govt intervention and regulation
Increase in mobility with new autonomous transf
Unable to distingush real and virtual world (fake identity, news, )
Reach the limit of ICT infrastructure capacity
AI Dominant
Big data Big companies
Surrounded by vulnerable AI Autonomous Things
Quantum initially only states but later
Quantum conputing
Cheap technology do not support adequate authentication identification authoriz
3D printing will be mainstream, also organic devices
More Like Cyborgs
Digital Divide
Difficult to attain trusted systems considering time to market
Hacking of phisical items
Too Large Attack Surface
Growth of Access to Transportation in develop. countries
Integration of new tech into old items
Certificated Sw
Internet o f fewer things -Use instead of owning - Virtualization
Surrounded by vulnerable AI Autonomous Things
Hacking of phisical items
Everything is a computer
You can be killed by a computer attack

# BECOME MEMBER!
# CONTACT US


European Cyber Security Organisation 10,
Rue Montoyer
1000 – Brussels – BELGIUM

www.ecs-org.eu

Phone:
+32 (0) 27770256

E-mail:
Ms. Eda Aygen
Head of Communications &
Advisor to the SecGen
eda.aygen@ecs-org.eu

Follow us
Twitter: @ecso_eu

# SWOT analysis for strategic priorities: Cybersecurity Technologies & Services, to protect important Infrastructure / Applications and citizens' privacy

### Risk Management: Predict, Prevent, Detect, Respond

EU legislations (GDPR, NIS, …) are going to structure and drive market growth (opportunity) with protection of critical infrastructure and privacy: EU has important positions in local, national and technology infrastructure (strength) but high fragmentation and sensitiveness issues are not facilitating exchange of information and improved management of cyber risks, from assessment to response (weakness) → need to establish technologies and platforms to increase risk management of infrastructure and key applications, complying with EU legislations (opportunities)

- **Security Assessment and Risk Management.**
- **Protection of innovative ICT infrastructure.**
- **Information Sharing, Security Analytics and Cyber threat Detection.**
- **Cyber threat management: response and recovery.**

### Increased data security for data-driven applications and services

EU technology competence in encryption, ID management and data protection as well as its approach to privacy (strength) should be continued to face continuous evolution of threats (threat) → secure data management at rest and in motion, considering privacy requirements will increasingly be requested by citizens and applications (opportunity)

- **Data security and privacy technologies.**
- **Quantum Resistant Crypto.**
- **Distributed Identity and Trust Management.**
- **User-centric Security and Privacy.**

### Resilient and user's acceptable architectures and tools for trusted solutions and services

EU position is strong in certain ICT technologies (strength) but is weak in many cybersecurity aspects that should protect those ICT solutions and applications (weakness): non EU solutions, not always sufficiently validated (threat) are used, also for costs reasons → need to better understand market needs and dynamics (opportunity) to develop EU solutions and innovative services (in particular from SMEs) and validate trusted supply chains.

- **Security and privacy by design.**
- **Trusted supply chain.**
- **Security services.**

# SWOT analysis for strategic priorities:
# Pilots and validation of solutions in Infrastructures & Applications

EU is world leader in several industrial applications, “conventional” key infrastructures and economic sectors (strength) but solutions are not sufficiently tested for the specific applications (or not known by users) and often not validated or certified for the specific applications (weakness). Users are still learning about the need to be protected from cyber threats (threat) → need for validation and pilot in the specific applications of solutions declined to the specific needs, to protect the economic sector or the critical infrastructure / services and promote EU innovative solutions (opportunity):

- **Industry 4.0 and ICS**
- **Energy, including Smart Grids**
- **Transportation**
- **Finance and Insurance**
- **Smart Cities & Smart Buildings**
- **Public Services / eGovernment / Digital Citizenship**
- **Healthcare**
- **Telecom, Media, and Content**

# SWOT analysis for strategic priorities:
# Cyber ecosystem: preparing the market to introduce and use innovations

The sustainable growth of EU economy and of the DSM, the digitalisation of the industry and the pervasiveness of ICT solutions and services at all level will face increased and distributed threats (threat). European countries have different approaches to prepare their citizens and professionals to these threats, but the maturity level to face threats and awareness of their potential impact is still considerably low (weakness). Standards are not sufficiently settled and certification is still fragmented in Europe (weakness). Innovation, particularly in services, is often coming from SMEs, but they are not sufficiently supported with instruments specific to this particular market → Education, training, awareness and exercises should be stimulated and supported at local and European level, possibly with increase harmonisation across countries to allow employment growth (opportunity) and increased cyber hygiene in users / citizens. EU certification (depending on the level of impact) would allow better trust in procurement and innovative business models (opportunity), in particular for SMEs.

- **Education and training.**
- **Simulation, cyber range and awareness.**
- **Certification and standardisation.**
- **High assurance prevention and protection.**
- **Digital instrument for SMEs.**

# SWOT analysis for strategic priorities: Cybersecurity Technologies & Services (Risk Management: Predict, Prevent, Detect, Respond)

- **Security Assessment and Risk Management.** GDPR and NIS directive will be important driving forces for EU DSM market development (opportunity), but non EU solutions are already present in the market (weakness). EU companies would improve their position on risk management solutions but there is still limited data sharing and limited understanding of implementation of possible solutions (weakness) → address timely the evolving and escalating threat environment and position EU solutions as reference at national and international level (opportunity)
  - *Integrated holistic methodologies for combined information security, cybersecurity, and reliability risk management resulting in reduced costs and improved efficiency for organisations and governments alike*

- **Protection of innovative ICT infrastructure.** EU is at the forefront of ICT infrastructure innovation, e.g. mobile, IoT (strength) delivering the expected DSM market growth (opportunity). The ICT infrastructure is becoming increasingly flexible and scalable but also more distributed and open to higher threats (threat) → the complex cooperation between multiple parties and the convergence of technologies such as cloud, network virtualisation, mobility, IoT should be supported to allow Europe to better control sensitive information exchange, protection of critical infrastructure and market growth (opportunity)
  - *High reliability and resilient ICT infrastructure enabling competitive advantages for European infrastructure solutions, e.g. networks and public clouds*

# SWOT analysis for strategic priorities: Cybersecurity Technologies & Services (Risk Management: Predict, Prevent, Detect, Respond)

- **Information Sharing, Security Analytics and Cyber threat Detection.** NIS directive as driving force for a structured market growth and DSM protection (opportunity), but Europe is still dependent on non-European solutions and data sources (weakness) → need to establish a trusted European threat intelligence for collaborative responses, leveraging advanced means of detecting system anomalies and integrity violations (opportunity)
  - *Comprehensive security analytics and threat intelligent technology integrated in a European platform for effective and timely co-operation resulting from fast sharing of information and dissemination of threat information on a high quality level*

- **Cyber threat management: response and recovery.** Compliance with GDPR and NIS directive as competitive edge for EU companies (strength & opportunity) but response and recovery tools are often poorly considered and / or integrated (weakness) → increasing demand of European technologies and services to recover and respond to cyber threats (opportunity)
  - *Integrated security infrastructure consisting of a reference implementation of a Response and Recover platform able to combat future threats*

# SWOT analysis for strategic priorities: Cybersecurity Technologies & Services (Increased data security for data-driven applications and services)

- **Data security and privacy technologies.** EU strong technical expertise to lead data protection (strength) but data security and privacy is a "moving target" (weakness) → need for continuous improvement of data management securing data at rest and in movement (opportunity)
  - *Secure and privacy aware data processing and storage with user friendly transparency and control*

- **Quantum Resistant Crypto.** EU unique expertise in post quantum cryptography (strength) but with long cyber innovation cycle (weakness) → need for a strategy to meet the challenges of quantum computing in terms of future threats and market opportunities (opportunity)
  - *Reduced window of unsafe cryptography and EU industry and governments well-prepared for the eventual appearance of quantum computers to preserve national security*

- **Distributed Identity and Trust Management.** Past investments put EU in a leading position on ID (strength) but existing systems do not fulfil the privacy-by-design requirements of eIDAS regulation (weakness) → with the need of distributed solutions and better authentication and authorisation approaches to benefit of the market growth linked to eIDAS and future legislative measures in the ID domain (opportunity)
  - *Increased trust in the cyber world and privacy-respecting identity management schemes with no single point of failure*

- **User-centric Security and Privacy.** Identity protection is a top priority in EU besides guaranteeing citizens rights and security, e.g. GDPR and privacy provision of eIDAS regulation (strength) but still low awareness level with citizens considered the weakest link (weakness) → need for risk management for individuals and user friendly security mechanisms (opportunity)
  - *Increased awareness and tools enabling user-centric security and privacy*

# SWOT analysis for strategic priorities: Cybersecurity Technologies & Services (Resilient and user's acceptable architectures and tools for trusted solutions and services)

- **Security and privacy by design.** EU has a strong reputation in privacy (strength) but sustainable efforts on cyber security and better knowledge of market dynamics are needed to keep up with the increasing cyberattacks (weakness) → need for methods and tools for developing secure software and hardware as well as metrics to validate users' acceptability and market opportunities (opportunity)
  - *Increased trust by both developers, that use the components as well by end-users and market stimulus for secure / privacy-friendly by-design solutions*

- **Trusted supply chain.** Despite ICT Leadership in key technologies and many diversified SMEs (strength) supply chains in Europe heavily depend on non EU solutions (weakness) → need for validation of trusted solutions and new methods for developing resilient systems out of potentially insecure components
  - *Increased trust along the supply chain and improved market opportunities for security component suppliers*

- **Security services.** EU has many diversified and innovative SMEs (strength) in security services but their market presence is not supported enough due to weak investments or difficult business models (weakness) → innovative services with advanced business models and collaborative approaches, in particular from SMEs providing or accessing security services (opportunity)
  - *Dynamic and innovative European market in cybersecurity services*

# SWOT analysis for strategic priorities:
# Pilots and validation of solutions in Infrastructures & Applications

- **Industry 4.0 and ICS.** European actors are leaders in ICS security (strength) and in several manufacturing sectors, but many deployed systems ICS components have usually very long lifetime and no sufficient security (weakness) → new infrastructure needs to be resilient and dependable to support the digitalization of the EU industry (opportunity)
  - *Convergence of safety and security tools and techniques in cybersecure developments (continuous risk assessment and monitoring) reaching societal acceptance and effective adoption, with new business models to support the positive impact of industry modernisation, employment growth and re-industrialisation of European countries*

- **Energy, including Smart Grids.** Europe commitment to prevent climate change and usage of renewable energy sources (strength) requires securing distributed energy resources for distributed users. This is increasing the attack surface over time (threat), with high level of complexity and volume of interconnected devices, integrated in long lifespans energy grids (weakness) → need new secure schemes for control and management to avoid cascading effects and major supply disruption (opportunity) particularly for energy distribution
  - *Security tools and techniques more efficient and more suited to increasingly distributed energy infrastructures needs and constraints to increase trust in security and safety*

# SWOT analysis for strategic priorities:
# Pilots and validation of solutions in Infrastructures & Applications

- **Smart cities and smart buildings.** Numerous EU policies and activities promote an integrated and more efficient approach to challenges in cities (strength) but the complexity of the threat landscape for smart cities and buildings need to be still understood and managed, better understanding also the increased challenges (weakness) linked to the inter-connectivity of smart systems → increased awareness of importance of safety and cyber resilience solutions for increased efficiency (opportunity)
  - *Transformation of cities legacy systems into a viable smart city concept with dynamic management of evolving and interconnected (to the different sectors) cyber security challenges, delivering high resilience, integrity, availability and privacy*

- **Transportation.** European automotive (but also railway and shipbuilding industry) is leading innovation worldwide in the transport sector (strength) but the increased connectivity of smart systems is making the attack surface larger (threat), with and increased need to guarantee safety and security in the long term (weakness) → cyber secure and validated technologies (linked to IoT solutions) and innovative mechanisms for connected / smart vehicles and autonomous systems are needed to allow deployment of new smart transport systems (opportunity)
  - *Convergence of advanced compliant and secure technology development in Europe and secure Europe's domestic and international transportation as an enabler for the continuing growth of the economic sector and safety of the individuals*

# SWOT analysis for strategic priorities:
# Pilots and validation of solutions in Infrastructures & Applications

- **Healthcare.** Deemed as one of the critical infrastructures for the citizens and the society, with huge presence of European manufacturers in the electronics health sector (strength), seamless electronic healthcare services require system availability, business continuity, and data security and integrity to improve services to citizens and reduce costs (opportunity) while facing increase of threat surface (threat) for data management and electronic connected devices (e.g. IoT based implants) → The market is still relatively new and fragmented in Europe (weakness) but the digitalisation of all the healthcare levels is needed to comply with the evolution of the society and cost reduction (opportunity)
  - *Digital autonomy in the healthcare sector and improved capability of eHealth services to automatically recover from cyberattacks, restoring the eHealth service level to its nominal status. Increased resilience of a national critical infrastructure*

- **eGovernment and public administration.** The Digital Agenda for Europe identifies open data as a driver for innovation, growth and transparent governance (strength) but public administrations still use legacy systems and have users with different security background (weakness) → the protection of local and public administration systems should be enhanced, cross-border data exchange between governments and private sector should be secured in EU in response to the growing economic and political awareness on impact of cyber threats and costs reduction of administrative services (opportunity)
  - *Increased citizens' trust in Governmental services, increased transparency, and economic efficiency*

# SWOT analysis for strategic priorities:
# Pilots and validation of solutions in Infrastructures & Applications

- **Finance and Insurance.** The ongoing regulation activities at the EU level for a DSM and harmonisation of different national frameworks (strength) need to be supported by actions to reduce systemic risks that cover the entire EU financial system and increase security and privacy protection (weakness) → use of validated secure technologies to enhance the resilience of the financial industry (opportunity)
  - *Perception of "Single European Digital Financial Market" as Cyber Secure and adoption of adoption of cutting edge innovative solutions to foster Data Protection, Data Integrity and Privacy*

- **Telecom, media, content.** EU Telecoms are major players on the world stage (strength) but the EU has a reputation of insufficient privacy protection and reliable high quality systems management (weakness) → large investments are needed in new technologies, e.g., network virtualization to allow the provision of new services at reduced cost (opportunity)
  - *Reliable telecommunication services, including cooperation of providers on security issues, and higher protections for clients*

# SWOT analysis for strategic priorities:
# Cyber ecosystem: preparing the market to introduce and use innovations

- **Education and training.** EU is promoting the DSM (strength) and the digitalisation of the society but there is still insufficient education / training to support the needed jobs related to this policy (weakness) → to cope with the increasing impact of cyber threats (threat) and needs from suppliers and users of specialised personnel (opportunity) it is urgent to share best practices in education & training and harmonise EU approaches to cyber hygiene
  - *Effective cooperation between academia and EU cyber security companies for a highly skilled workforce able to respond flexibly to dynamic requirements; improvement of citizens behaviour in the digital world*

- **Simulation, cyber range and awareness.** EU world leader in several industrial applications (strength) and while industry digitalisation is progressing (opportunity), there is still a low cybersecurity competence and awareness at professional level (weakness) → the workforce needs training and exercising in tackling cyber security issues and face the high complexity as well as the evolution of new IT systems and infrastructure, making them resilient and dependable (strength); citizens needs increased awareness to avoid threats and decision makers needs to take informed decision to implement solutions
  - *Impact on security assessment and risk management, including cyber risk governance (safety vs security analyses, impact analysis, insurance) and enabled informed decisions on security-related investments at the corporate and national level.*

# SWOT analysis for strategic priorities:
# Cyber ecosystem: preparing the market to introduce and use innovations

- **Certification and standardisation.** Ongoing policy activities at the EU level (strength) are addressing fragmentation (weakness) at EU and national level in standardisation → need for different levels of trusted products and services for the large European market (opportunity) thanks to a transparent and harmonized certification mechanism which will help innovation to better enter the market (opportunity), addressing technical and human requirements and national regulations
  - *Defragmentation of the European Cybersecurity market thanks to better uptake of (innovative) security products and services while generating trust and confidence sustained by higher awareness of security and privacy along the complete value chain, also improving business models and procurement decisions*

- **High assurance prevention and protection.** Strong EU scientific and technical expertise (strength) but long cyber innovation cycle (weakness) → address the internal demand and the evolution of infrastructures and applications (opportunity)
  - *Increase the trustworthiness of European ICT services and products and competitiveness of industry and protection of EU fundamental rights of privacy and data protection*

- **Digital instrument for SMEs.** EU has many innovative and diversified SMEs (strength) but they hardly bring innovation to market or have difficulty to cooperate with users (weakness) → need action to help them addressing cybersecurity challenges, bosting their innovation capacity (e.g. disruptive technologies, dynamic services) but also helping them in market knowledge and economic resources in a more coordinated and structured way (opportunity)
  - *Increased cybersecurity services from and for SMEs with a sustainable ecosystem and increased business opportunities and users' knowledge of their solution, also via strong cooperation with large companies (suppliers and users)*