EUROPEAN CYBER SECURITY ORGANISATION

Moving towards a trustworthy and resilient European cyber secure ecosystem

Roberto G. Cascella (ECSO Secretariat)

European Industry Partnerships for New Digital Age Collaborative Event

Session on ”Secure Trusted Data/Knowledge – Applications and Infrastructure"

– 12 September 2019 – Brussels (Belgium) –

European Commission

ECS
EUROPEAN CYBER SECURITY ORGANISATION

We are the European Commission's partner in implementing the contractual public-private partnership (cPPP) on cyber security, established in 2016.
€ 500 mln from the EC for H2020 R&I projects (2017-2020), leverage factor > 3.

We unite and represent European cyber security industry players, as well as national public administrations, research centres, SME's and regions and academia

Our membership has grown from 132 members in June 2016 to more than 250 members in June 2019 (reaching out 2000 stakeholders)

ECSO definition of European Cyber Security

"European Cyber Security is our

common science, knowledge, trustworthy processes, products, services and infrastructures

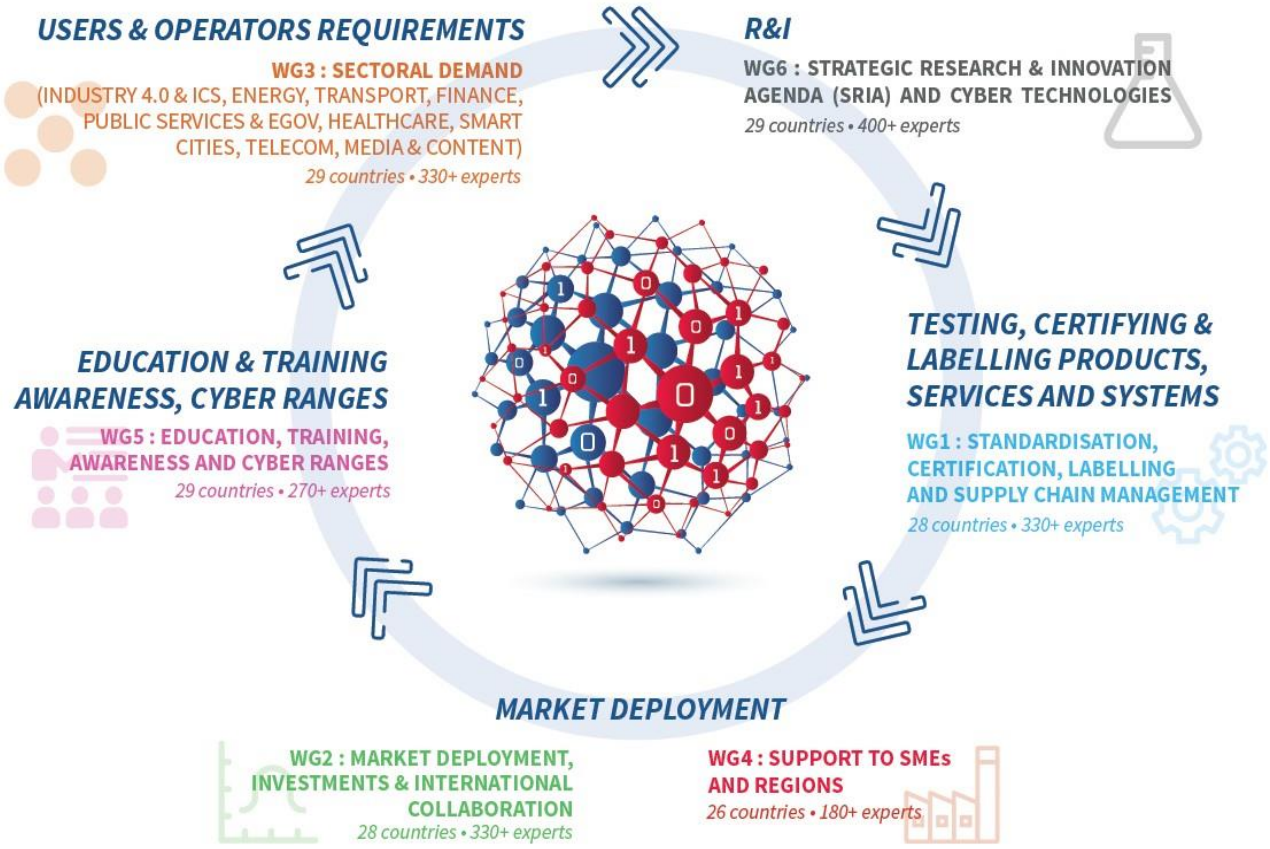
to protect (in a sustainable way)

our nations, industries / economies, citizens and institutions

against damaging cyber-attacks

while respecting our European Values."

ECSO Working Groups – cybersecurity 360°



WG6 mission

Define the cyber security **R&I roadmap** to strengthen and build a resilient EU ecosystem by designing and developing **trusted technologies** that address the **challenges of digitalisation** of the society and industrial sectors to foster EU **digital autonomy**

ECSO WG6: SRIA and Cyber Technologies

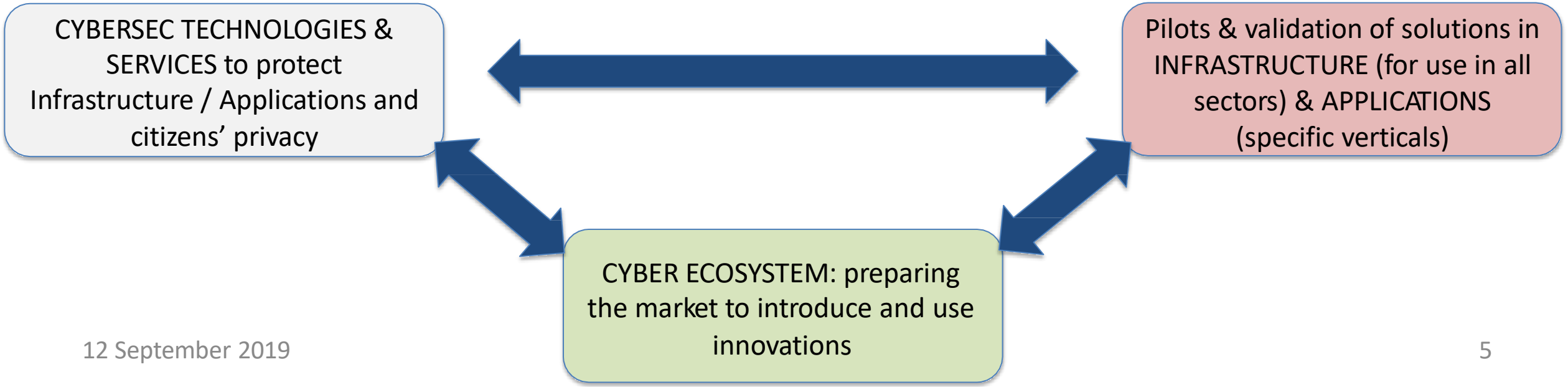
ECSO SRIA to identify research priorities for 2018-2020

è A strategic vision is needed to demonstrate how industrial priorities contribute to the implementation of the strategy

Analysis of the Work Programme 2018-2020 and continuous advocacy of priorities

è good match and public & private priorities well aligned

1 European Ecosystem for cyber security
2 Demonstrations for the society, economy, industry and vital services
3 Collaborative intelligence to manage cyber threats and risks
4 Remove trust barriers for data-driven applications and services
5 Maintain a secure and trusted infrastructure in the long-term 6 Intelligent approaches to eliminate security vulnerabilities in systems, services and applications
7 From security components to security services



Moving forward in supporting the EU ecosystem

- **Analysis of global trends to define the strategy through 2027 (SRIA 2.0)**
- **Technical papers** (under preparation)
  - Artificial Intelligence, Internet of Things and Blockchain
  - New ones planned on “5G and communication technologies” & “Post-quantum crypto”
- **Global vision for future EU cybersecurity**
  1. Impact for Society and Citizens (Social Good)
  2. Digital Transformation in Verticals
  3. Data and Economy
  4. Basic and disruptive technologies
- Contribution from ECSO with **priorities for Horizon Europe and the Digital Europe Programmes**
- **Collaboration with other cPPPs** to federate the discussions on cybersecurity challenges
  è Cybersecurity as a glue and horizontal technology

Present and future opportunities / challenges

- **Autonomous systems** (cars, trains, drones, delivery, robotics, medical diagnostics)**:** will change our lives and business models
- **Mass transportation** vehicle likely initially more impacted than personal cars
- **Constant monitoring of many aspects of our life**: huge (and sensitive) data storage (local storage becoming obsolete)
- **Self-sustaining mobile devices** (thanks to microelectronics and battery technologies)
- **5G networks** will support growth of mobility and industrial development
- Massive presence of **IoT and IIoT** will impact supply chain and logistics with automatic decisions and real time adaptable
- **Additive manufacturing and 3D printing** enabling to create "everything everywhere"
- Expected **major cyber attacks** to critical infrastructure elements ("Cyber Pearl Harbour")
- Massive **fake news will fundamentally stress democratic** rights and will distort views of reality for citizens à "Trust" could become an obsolete word
- **Quantum computers** will break traditional crypto and dramatically increase access to encrypted data
- High use of **digital twins** (digital replica of a living or non-living physical entity) also as means to secure cyber physical systems
- **AI capabilities** will provide a large portion of **decisions about systems, humans and society**
- AI will lead to significant **improvement of parts of cyber and physical security provisioning process**

Key Technologies - future basic and disruptive technologies, for the digital society: what future?

- **Quantum computing and post-quantum cryptography** (a help and a threat to cyber security)
- **Artificial Intelligence and cognitive science** (an enabler to anticipate and understand threats, but also a potential cyber weapon)
- **5G and new disruptive communication networks** (a technological, economic and political challenge)
- **Internet of Things and Cyber Physical systems** (tens of thousands of connected objects: how to make them safe?)
- **Blockchain and Distributed Ledger Technologies** (from bitcoin to use in a growing number of applications)
- **Robots and cyborgs** (support to growth or threat, in particular when coupled to AI?)
- **Digital Twins**
- **Biotechnologies and augmented human** (computing, communication, etc.)

Building and strengthening the EU ecosystem – Social Good –

- Need to develop **resilient** systems, including software, with a **security by design** approach to reduce the financial impact of zero-day attacks
- Definition of **risk management strategy** and countermeasures to manage **future unknown (evolving) attacks** or fast-adaptable attacks
- **Vulnerability management** and development of tools to support cybersecurity assessment, evaluation and certification
- Measures for a **trustworthy supply chain**
- **Cyber range** technologies and services including sector specialisation
- Trust mechanisms in the **machine economy**
- **Cyber-augmented** humans

Cyber resilient infrastructures and services – Digital transformation in verticals –

- Enhance the security level of **highly critical infrastructure**, including, energy (electricity, gas, oil), water distribution, telecommunications, etc.
- **Threat intelligence** and **situational awareness** to improve the reaction to cyber incidents
- Increase **trust** in the 4th industrial era to reduce the impact of cyber threats on business continuity
- Develop **cyber secure communication** systems and **networks of the future**
  - High complexity due to convergence (5G, IoT, Cloud) at the infrastructure level and convergence of different technologies (Virtualisation, Artificial Intelligence, SDN, etc…)
- **Security orchestration** in heterogenous systems and networks
  - End to end security, and not only network security!
  - Time dimension to be considered

Data one of the key drivers for our digital economy – Data and economy –

- Provide the foundations for a **trustworthy and reliable data-driven economy** of the future
- Support the needs of digital services with **new privacy-preservation techniques** to protect the economic growth and European digital transformation
- Provide tools and mechanisms for supporting the processing, mining and dissemination of personal data and models with privacy guarantees
- Verify the correctness of the information to increase trust in digital services (handle fake news)

Building blocks to develop a secure & resilient DSM – Basic and disruptive technologies –

ECS
ROPEAN CYBER SECURITY ORGANISATION

- Models to define and validate security properties for **AI-driven systems**
- **Trustworthy AI-based systems** to increase trust in the decision process
- Security guarantees along the product chain, from hardware implementation to product deployment and service delivery
- Technologies for **trusted electronics** and continuously assessment of their quality and security
- **New cryptographic area** (schemes and systems)
- Procedures for the **secure evaluation** and efficiently implement cryptographic algorithms
- Design new digital-based, secure and **privacy-friendly cryptocurrency**
- Address **IoT challenges** at all layers in the stack (device, connectivity, platform and application), and a across different layers or IoT systems as a whole.
- Design a new family of **cyber-aware and adaptive applications**

Clustering of strategic developments to increase digital autonomy

Crypto and data protection	• Technologies and solutions for cryptography • Blockchain / DLT for different applications • Secure Digital Identities & Root of Trust • Solutions for trusted / confidential information sharing • Technologies and solutions for secure data lifecycle • Security for data analytics
Trustworthy IoT technologies/devices	• IoT security / Cyber Physical Systems • Trustworthy and secure personal devices on a secure core
Secure Operating Systems and dependable platforms	• Open source operating systems • High Performance / Quantum computing • Trusted and secure European data management infrastructure (at rest and in motion)
European Internet and resilient 5G networks	• 5G security (end to end) • European trusted and secure routers è Secure Network Function virtualization
Collaborative intelligence to manage cyber threats	• Artificial Intelligence / Machine Learning (also for autonomous management – self-healing) / Big Data Analytics • Multi-sovereign probes development and deployment • European trusted Intrusion Detection System (IDS) for function, equipment and services • European trusted Security Information and Event Management (SIEM) solutions • Technologies and solutions for incident response • Advanced SOCs (Security Operation Centres) and Cybersecurity control centres (connected across EU) • Technologies and solutions for threat intelligence and cyber range
Assurance, Certification for a trustworthy cyber ecosystem	• Tools for validation of Products & services certification • EU / national validation platforms also for Software Security Assessments • EU cybersecurity academia; education and training at national / regional / local level

➢ Analysis of national strategies
➢ Risk assessment methodology for third party technology
Ø Analysis of the impact for vertical sectors

Importance of large pilot projects

Areas of strategic investment for capability development

Support to policy implementation

Support to technology development

- Trusted network infrastructure strategic for the development of resilient application domain services
- Better understanding of potential vulnerabilities to anticipate cross-platform attacks
- Self-Sovereign Identity, Blockchain, user-centric, privacy-respecting identity and access control ecosystems
- Intelligent platforms for verification and decision making
- Secure software development and platforms for trusted electronics
- Migration Strategies for Quantum-Resistant Crypto

Support to competitiveness and market development

Support to competence building

BECOME MEMBER!
CONTACT US

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

www.ecs-org.eu

Phone:
+32 (0) 27770252

E-mail:
Dr. Roberto G. Cascella
Senior Policy Manager
roberto.cascella@ecs-org.eu

Follow us
Twitter: @ecso_eu