

Fabio Martinelli (CNR) cPPP Cyber Security (ECSO) and its SRIA

Outline of presentation:

- Description of the cPPP in cyber security
- Current elements of SRIA
- Some elements possibly useful for Smart Networks and Services

Short bio:

- *Fabio Martinelli* is a research director of the **Italian National Research Council (CNR)**, where He manages the Cyber Security Lab
- His main research interests involve security and privacy in distributed and mobile systems and foundations of security and trust.
- He is project coordinator of the **EU Network on Cyber Security (NeCS)** and of the Collaborative information sharing and analytics for cyber protection (C3ISP) project.
- He serves as Vice-Chairman of the Board of the European Cyber Security Organization (ECSO) and He is co-editor of the ECSO SRIA and serves in the partnership Board
- btw, He also serves in the executive committee of the Cyber Security competence centre of **Tuscany Region**



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 (2BE initiative).

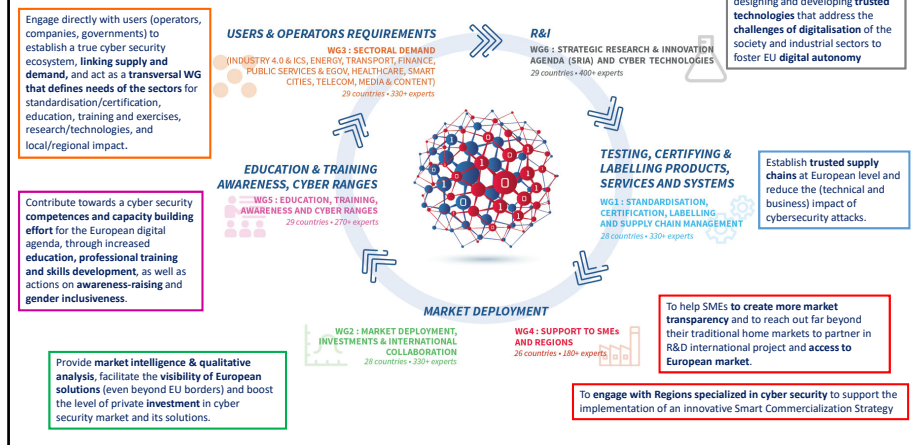


We unite and represent European cyber security industry players, as well as national public administrations, research centres, SME's and regions and academia



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

ECSO Working Groups – cybersecurity 360°



WG6 – Strategic Research and Innovation Agenda (SRIA) and cyber technologies

NEW WG6 ORGANISATION: Current WG6 activities largely focus on the definition of R&I priorities

- **SWG 6.1 "Ecosystem"**
- **SWG 6.2 "Digital Transformation in Verticals"**
- **SWG 6.3 "Data and Economy"**
- **SWG 6.4 "Basic and Disruptive Technologies"**
- **SWG 6.5 "Cybersecurity for Defence"**

REPORTS & STRATEGIC DOCUMENTS

- **Technical papers on Artificial Intelligence, Internet of Things and Blockchain** (first half 2019). New ones planned on "5G and communication technologies" & "Post-quantum crypto"
- **Vision papers on cyber security priorities towards Horizon Europe** (ECSO 2021-2027 vision): ongoing activity.

COLLABORATIONS

- **cPPPs (BDVA, euRobotics, EFFRA, A.Spire, 5G, AIOTI):** the ECSO technical papers will be used to continue the collaboration with the cPPPs. A joint paper will be proposed where cyber security will be the glue factor to present common challenges with all relevant cPPPs. Interest from several cPPPs in the initiative, during common or events where ECSO has been invited to discuss the cooperation. Other initiatives (ECSEL) contacted.
- **WG6 continues collaboration with EDA** on Agency's research priorities and with **ENISA** on the research priorities identification (crystal ball).

NEXT STEPS

- Finalise the technical papers and vision documents for initial priorities. Work on a specific context case for cybersecurity for defence

WG6 Strategy & Actions

Main building blocks to achieve the objectives and activities

Identification of R&I priorities (HorizonEurope and DEP) and alignment with industrial needs

- Monitor of H2020 projects and results
- Technical papers on cyber technologies and impact on vertical sectors
- Identification of key trends and predictions
- Market analysis and investments to determine cyber security challenges in short- / medium- / long- term
- Collaboration with other cPPPs and initiatives

Digital Autonomy: investments and relevance

- Identification of key technologies and solutions (cybersecurity and cyber defence)
- Analysis of national strategies
- Risk assessment methodology for third party technology
- Analysis of the impact for vertical sectors

Support the implementation of key legislations and directives

- Needs for certification and Cybersecurity Act
- Artificial intelligence and liability (via technical papers)
- GDPR and impact on new technology (via technical papers)

Coordinated cyber security strategy across sectors and domains

- Coordination with BDVA and EFFRA initiated and well established
- Collaboration with 5G PPP under development
- Collaboration with ECSEL, EURobotics, Photonics, A.Spire
- Collaboration with EDA on Cybersecurity for Defence (dual use technologies)
- Collaboration with ENISA

Coordination with cyber security pilot projects

- Technical coordination of industrial challenges and roadmaps (also measures for certification, training and skill creation)
- Community building and governance models

WG6 highlights on ongoing activities

- **Technical papers** under preparation on:
 - Artificial Intelligence, Internet of Things and Blockchain (first half 2019).
 - New ones planned on "5G and communication technologies" & "Post-quantum crypto"
 - Others under consideration
- **Cooperation with other cPPPs:** cybersecurity is transversal
 - MoU with 5G IA
- Identified a **global vision for future EU cybersecurity**, split in 4 areas: Impact for Society and Citizens (Social Good); Digital Transformation in Verticals; Data and Economy; Basic and disruptive technologies
- Contribution from ECSO with **priorities for Horizon Europe and the Digital Europe Programmes**
- **Identification of key technologies and solutions**

6

Technical Paper on Blockchain

Introduction to Blockchain

- A Disruptive technology that opens new possibilities for improving many services and even offers the possibility for the creation of new ones and new business models
- Even though the possibilities are enormous, its knowledge and application are still in the preliminary stage. 2 different points of view: Traditional and Disruptive

→ Blockchain as a technology that (i) can solve certain cybersecurity issues and (ii) needs to be properly secured

Some cyber security challenges

- Cryptocurrency economy and cryptojacking
- Data integrity & availability
- Global identity of users and devices
- Security and integrity of software/firmware and log files
- Data sovereignty
- IoT security and blockchain (P2P communication)
- Cyber Threat Intelligence (secure synchronization between different information systems)
- Traceability and transparency of processes



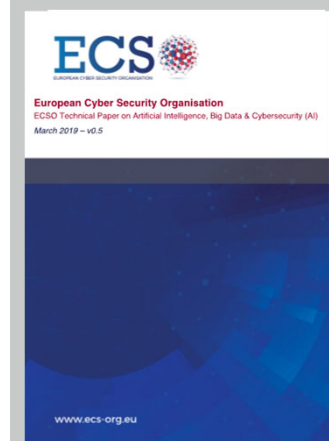
Technical Paper on Artificial Intelligence

Introduction to Artificial intelligence

- A Disruptive technology that is a subfield of computer science and it refers to any technique which enables computer to mimic human brain manifesting intelligence.
- Artificial Intelligence and Cyber security: a tight link:
 - Deep understanding of AI vulnerabilities that may allow an attacker to subvert the output of the system.
 - Artificial intelligence could be used and even be more efficient to attack a system rather than protecting it.
 - AI as a defensive technique

Some cyber security challenges

- Privacy-aware big data analytics/data mining.
- Big data secure storage
- Trust and big data
- Big data analytics and AI for security
- Secure protocols for big data processing
- Provenance of big data
- Protection against internal and external data theft
- Adversarial machine learning
- Machine learning for cyber security
- Model cloning (protection of the AI model)
- Ethical and legal aspects (explicable AI for cyber security)



Technical Paper on IoT

Introduction to Internet of Things

- IoT is a central element in the global digitalisation trend that is reaching our industry, our economy and our society.
- The key to success is the adequate implementation (secured and trustable) of technical enablers that should be addressed to enable IoT cybersecure deployment: physical devices, connectivity and networking, IoT platforms and services, and IoT applications.

Some cyber security challenges

- At device level
 - Secure execution
 - Firmware and application integrity, and updates delivery.
 - Protection against advanced physical attacks
 - Protection against micro-architectural attacks
 - Secure migration to post-quantum cryptographic algorithms
- Connectivity and network layer
 - Security and privacy of data
 - Transition to edge computing
 - Secure key management
 - Secure routing, cryptography, network level privacy
- IoT platform and IoT service layer
- Application layer and related to end-users Big data analytics and AI for security
- Cross-cutting



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, but will introduce large "attack surface" to cyber threats and little patching capability
- 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 (also with the support of social media). "Trust" could become an obsolete word.
- Quantum computers** will break traditional crypto and dramatically increase access to encrypted data: will post-quantum crypto provide some security?
- Cryptocurrencies** will proliferate
- High use of **digital twins** (digital replica of a living or non-living physical entity) also as means to secure cyber physical systems
- Citizen science to tackle complex security issues that could be exploited to prevent attacks and make the systems more resilient
- AI capabilities** will provide a large portion of **decisions about systems, humans and society to be done by algorithms instead of humans.**
- AI will lead to significant **improvement of parts of cyber and physical security provisioning process.** On the other hand, the same development will **empower the attackers and contribute to a great number of novel and extended security threats**

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

Key technologies for the future and their link to cyber security:

- 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.)

Clustering of strategic developments to increase digital autonomy: investments and relevant topics

Crypto and data protection	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> IoT security / Cyber Physical Systems Trustworthy and secure personal devices on a secure core
Secure Operating Systems and dependable platforms	<ul style="list-style-type: none"> Open source operating systems High Performance / Quantum computing
European Internet and resilient 5G networks	<ul style="list-style-type: none"> 5G security (end to end) European trusted and secure routers → Secure Network Function virtualization
Assurance, Certification for a trustworthy cyber ecosystem	<ul style="list-style-type: none"> 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
	<ul style="list-style-type: none"> 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
 - Analysis of the impact for vertical sectors
- Importance of large pilot projects**


Some cybersecurity challenges for future communication networks

- High complexity
 - Convergence of IoT, Cloud and 5G at the infrastructure level
 - Convergence of different technologies: Virtualization, Artificial Intelligence, SDN, etc...
 - Serving diverse applications, also critical and strategic services
- Large attack surface (also due to the use of new technologies)
- Continuous evolving systems
 - Orchestration of the security needs to be fully integrated with the orchestration of the network
- End to end security, and not only network security!
 - Network and application security coupling
- Multi-tenant and complex access control management
- Need and opportunity for Data Sharing, Data Usage control (including obligations management)
- ...

13

CONTACT

Fabio.Martinelli@iit.cnr.it

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

www.ecs-org.eu

Phone:
+32 (0) 27770250

E-mail:
secretariat@ecs-org.eu

Follow us
Twitter: [@ecsso_eu](https://twitter.com/ecsso_eu)

